TLP: CLEAR

RETAIL & HOSPITALITY INDUSTRY INSIGHTS

2024 Verizon Data Breach Investigation Report Analysis

RETAIL & HOSPITALITY ISAC

Introduction

With 270 member companies from the retail, hospitality, and travel industries, the threat intelligence shared by our RH-ISAC membership is an excellent representation of the trends prevalent in our sector. We wanted to know how our data compared to other sources tracking retail cyber trends. Every year, cybersecurity researchers at Verizon release a Data Breach Investigation Report (DBIR) with an in-depth quantitative analysis of the cyber threat landscape broken down by attack type, region, and industry. Verizon researchers found their retail, accommodation, and manufacturing sectors faced many of the same threats that our members reported: credential stealing, ransomware, and phishing targeting sensitive data for financial gain.

This report compares some of the key takeaways from the Verizon Report with our own member data, providing additional context to help you benchmark your threat landscape against a wider community of your peers.

RH-ISAC member reporting and sharing largely confirms the trends identified by Verizon, with credential harvesting, ransomware, and phishing representing the largest share of threats facing the community. However, RH-ISAC data tracking provides significantly more specific details for the community threat landscape, such as specific malware families targeting members. The advanced capabilities of the RH-ISAC MISP instance also allow us to examine in more granularity the threat actors and tactics, techniques, and procedures facing the RH-ISAC community. Major emerging trends for 2023 across industries included the explosion of vulnerability exploitation in third-party breaches and the adoption of artificial intelligence (AI) by threat actors.

Executive Summary

As in 2023, RH-ISAC analysts reviewed the Verizon DBIR report and compared the findings to sharing data from the retail, hospitality, and travel communities. Key points of comparison were:

- Phishing, ransomware, and credential harvesting remained top threats, identified in both the Verizon data and in RH-ISAC reporting data
- DDoS attacks remained a high area of focus for Verizon but did not show as prevalent in RH-ISAC reporting
- Vulnerability exploitation rose significantly as an initial infection vector, according to the Verizon report, and while the RH-ISAC community discussed this trend heavily, it did not emerge as a top identified threat
- Third Party Risk was a key trend in both the Verizon report and in RH-ISAC community concerns
- While Business Email Compromise (BEC) remained a key trend in the Verizon report, for the RH-ISAC community BEC was a small part of a larger fraud threat landscape that emerged as a key concern
- The Verizon report noted that threat actors increasingly leveraged generative artificial intelligence to innovate fraud methodologies, which was a key topic for the RH-ISAC community as well

For comparison, key points of comparison from the report covering 2022 were:

- Phishing, ransomware, and credential harvesting were key top threats reported and discussed in the RH-ISAC community, which aligns with top threats in the Verizon DBIR
- Denial-of-Service (DoS) attacks, while present, did not rank as a key threat reported or discussed by the RH-ISAC community, as opposed to being a top threat in the Verizon DBIR
- Member discussion of BEC attacks on sharing platforms increased over 2022, corresponding to the massive increases noted by Verizon
- Members focused heavily on defending against the Log4j vulnerability throughout the first half of 2022, aligning with defense activity reported by Verizon, which slowed as the industry moved to patch quickly
- Attacks targeting customer payment data are among the top concerns for RH-ISAC members, which aligns with the granular view of industry-specific metrics provided by Verizon

KEY TAKEAWAYS: 2024 Verizon DBIR

Key Trends for Retail, Hospitality, and Travel

For the retail, hospitality, and travel sectors, RH-ISAC reviewed the Verizon report and identified the key trends and findings most relevant to the community and the key industries listed that most closely align with our community sectors.

Most common attack method: stolen credentials, phishing, and vulnerability exploits

Most commonly targeted data: personally identifiable information (PII), credentials, and internal data

Most prevalent threat: 91% of industries saw ransomware in the top 3 most prevalent threats

Ransomware: 24% of all breaches

Social engineering: 50% of social engineering attempts involved pretexting: the fabrication of scenarios to pressure victims into divulging sensitive information

External vs. internal: 83% of breaches originated from external actors

Motivation: 95% of breaches were financially motivated

Log4j: major concern for cyber defenders across multiple industries, with 90% of vulnerability exploit incidents referencing Log4j

Most prevalent threat actor type: organized crime

Key MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs): social engineering, denial of service, system intrusion, and basic web application attacks

Key Developments

Major new findings for the current report marking differences from prior reports include:

- 2023 saw the most breaches by volume of all previous years surveyed
- Vulnerability exploitation, especially in third party suppliers and vendors, increased drastically
- Ransomware tactics shifted significantly to extortion over encryption

Key Industries

Key changes in most targeted industry rankings by incident count included:

- Accommodation and Food Service incidents dropped from 254 incidents to 220, while confirmed breaches rose from 68 to 106
- Agriculture incidents rose from 66 incidents to 79, while confirmed breaches rose from 33 to 56
- Entertainment incidents rose from 432 incidents to 447, while confirmed breaches rose from 93 to 306
- Manufacturing incidents rose from 1,814 incidents to 2,305, while confirmed breaches rose from 259 to 849
- Retail incidents rose from 404 incidents to 725, while confirmed breaches rose from 191 to 369
- Transportation incidents dropped from 349 incidents to 260, while confirmed breaches rose from 106 to 138
- Wholesale Trade incidents dropped from 96 incidents to 76, while confirmed breaches rose from 53 to 54

For comparison, the key findings for 2022 were:

Key Findings Comparison

Across all industries surveyed, Verizon reported core metrics and trends:

- Stolen credentials and phishing were by far the most prevalent infection vectors
- Stolen credentials were used in one third of all breaches
- Attacks involving the exploitation of vulnerabilities to initiate a breach increased 180% from 2022
- One third of all breaches were ransomware incidents, and ransomware was the top threat for 92% of industries
- Ransomware attacks largely pivoted from encryption-based methodology to solely extortion
- 68% of breaches involved human error, toughly the same as 2022
- Third Party breaches represented 15% of all incidents
- Business email compromises (BEC) accounted for 1/4 of financially motivated attacks

Metrics & Trends by Industry

Verizon provided a deep dive on findings for a few key industries, included below:

	Incidents & Breaches	% of Breaches Executed by External Actors	% of Attacks Financially Motivated	Primary Targeted Data	Notable Trends
Accommodation & Food Services	220 Incidents 106 Confirmed Breaches	92%	100%	Credentials - 50% Personal - 28% Payment - 19% System -19% Other - 16%	92% of breaches: System Intrusion Social Engineering Basic Web Application Attacks
Manufacturing	2,305 Incidents 849 Confirmed Breaches	73%	97%	Personal - 58% Other - 40% Credentials - 28% Internal - 25%	83% of breaches: System Intrusion Miscellaneous Errors Basic Web Application Attacks
Retail	725 Incidents 369 Confirmed Breaches	96%	99%	Credentials - 38% Other - 31% Payment - 25% System - 20%	92% of breaches: System Intrusion Social Engineering Basic Web Application Attacks

Metrics & Trends by Geography

Verizon also provided key data for several geographic regions:

	Frequency	Top Patterns	Threat Actors	Actor Motives	Data Compromised
Asia-Pacific	2,130 Incidents 523 with confirmed data disclosure	95% of breaches: System Intrusion Social Engineering Basic Web Application Attacks	External - 98% Internal - 2% (breaches)	Financial - 75% Espionage - 25% (breaches)	Credentials - 69% Internal - 37% Secrets - 24% Other - 17% (breaches)
Europe, Middle East, and Africa	8,302 Incidents 6,005 with confirmed data disclosure	87% of breaches: Miscellaneous Errors System Intrusion Social Engineering	External - 51% Internal - 49% (breaches)	Financial - 94% Espionage - 6% (breaches)	Personal - 64% Other - 36% Internal - 33% Credentials - 20% (breaches)
North America	16. 619 Incidents 1,877 with confirmed data disclosure	91% of breaches: System Intrusion Social Engineering Basic Web Application Attacks	External - 93% Internal - 8% (breaches)	Financial - 97% Espionage - 4% (breaches)	Personal - 50% Credentials - 26% Internal - 19% Other - 16% (breaches)

This data shows key increases for each region:

- Incidents in the Asia-Pacific (APAC) region nearly doubled from 699 to 2,130, with confirmed breached increasing from 164 to 523
- Incidents in the Europe, Middle East, and Africa (EMEA) region also increased exponentially from 2,557 to 8,302, with confirmed breaches increasing from 637 to 6,005
- Incidents in the North America (NA) region also increased significantly from 9,036 to 16,619, with confirmed breaches increasing from 65 to 1,877

KEY TAKEAWAYS: RH-ISAC

Sharing data from the RH-ISAC membership shows interesting comparisons with the Verizon DBIR data. The most notable points of comparison are:

Top Threats

Phishing, ransomware, and credential harvesting remained top threats, identified in both the Verizon data and in RH-ISAC reporting data

DoS Attacks

DDoS attacks remained a high area of focus for Verizon but did not show as prevalent in RH-ISAC reporting

Vulnerability Exploitation

Vulnerability exploitation rose significantly as an initial infection vector, according to the Verizon report, and while the RH-ISAC community discussed this trend heavily, it did not emerge as a top identified threat

Third-Party Risk

Third Party Risk was a key trend in both the Verizon report and in RH-ISAC community concerns

GenAI

The Verizon report noted that threat actors increasingly leveraged generative artificial intelligence to innovate fraud methodologies, which was a key topic for the RH-ISAC community as well

Business Email Compromise (BEC)

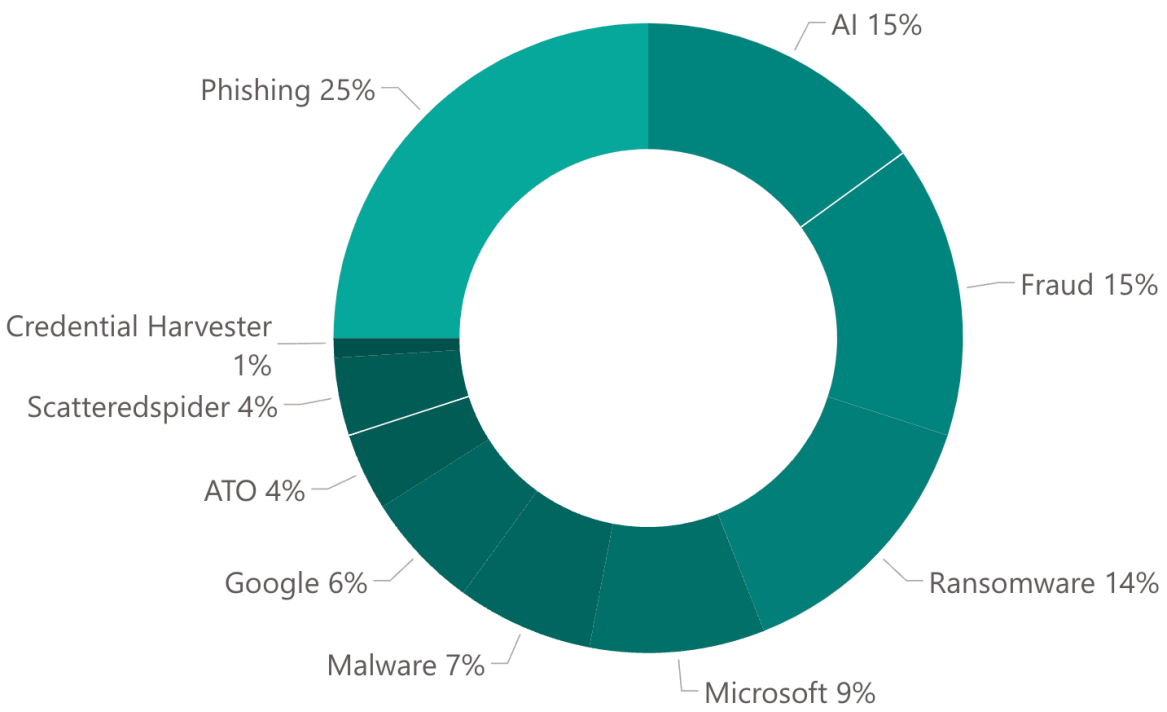
While Business Email Compromise (BEC) remained a key trend in the Verizon report, for the RH-ISAC community BEC was a small part of a larger fraud threat landscape that emerged as a key concern

For comparison, the key points of comparison for 2022 were:

- Phishing, ransomware, and credential harvesting were key top threats reported and discussed in the RH-ISAC community, which aligns with top threats in the Verizon DBIR
- DoS attacks, while present, did not rank as a key threat reported or discussed by the RH-ISAC community, as opposed to being a top threat in the Verizon DBIR
- Member discussion of BEC attacks on sharing platforms increased over 2022, corresponding to the massive increases noted by Verizon
- Members focused heavily on defending against the Log4j vulnerability throughout the first half of 2022, aligning with defense activity reported by Verizon, which slowed as the industry moved to patch quickly
- Attacks targeting customer payment data are among the top concerns for RH-ISAC members, which aligns with the granular view of industry-specific metrics provided by Verizon

2023 Top Sharing Trends

This graph illustrates the RH-ISAC community's shared threat trends for 2023, which can be described as the frequency that threats were shared through Member Exchange, Slack, and the Core Member Listserv.



For comparison, in 2022, key trends included:

- Credential harvesting overtook phishing as the topmost shared threat topic in 2022, at 49%
- Phishing dropped from first place in 2021 to second place with 23%
- Agent Tesla reporting rose from fourth place in 2021 to third with 9%
- Log4j did not make the list of top shared threats for 2022, reflecting the sharp drop off in reporting as organizations moved quickly to patch
- The remaining threats on the list include tools and threat groups well known to cyber defenders such as: Formbook (up to 4th place with 4% from 6th place in 2021), Emotet (at 5th place with 4% after not making the list for 2021), and SocGholish (at 6th place with 3% after also not making the list in 2021)

As with 2022, the Top Shared Trends for 2023 largely corroborate Verizon's primary findings that phishing and credential-stealing are among the most prominent initial infection threats facing organizations in the retail, hospitality, and travel sectors.

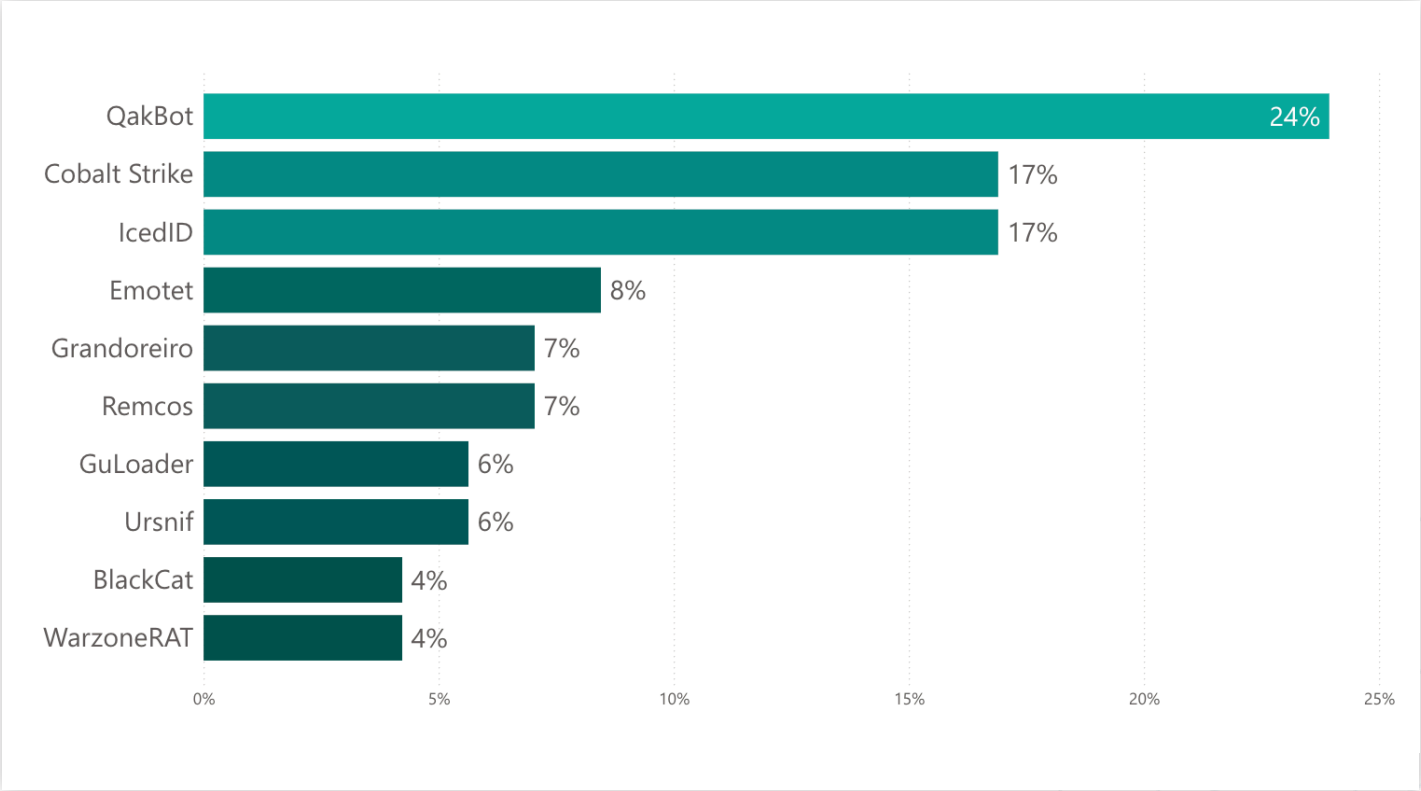
TOP MISP SHARING THEMES in 2023

For the period of January 1, 2023 through December 31, 2023, members published 2,568 events to MISP, including 50,199 unique attributes, compared to 1,348 events and 18,591 attributes in 2022. Key trends in MISP sharing are detailed below:

For the period of January 1, 2022 through December 31, 2022, members published 1,348 events to MISP, including 18,591 unique attributes. Key trends in MISP sharing are detailed below:

Top Malware and Tools

The following graph demonstrates the most common malware and tools (defined as ATT&CK Software) reported by members:

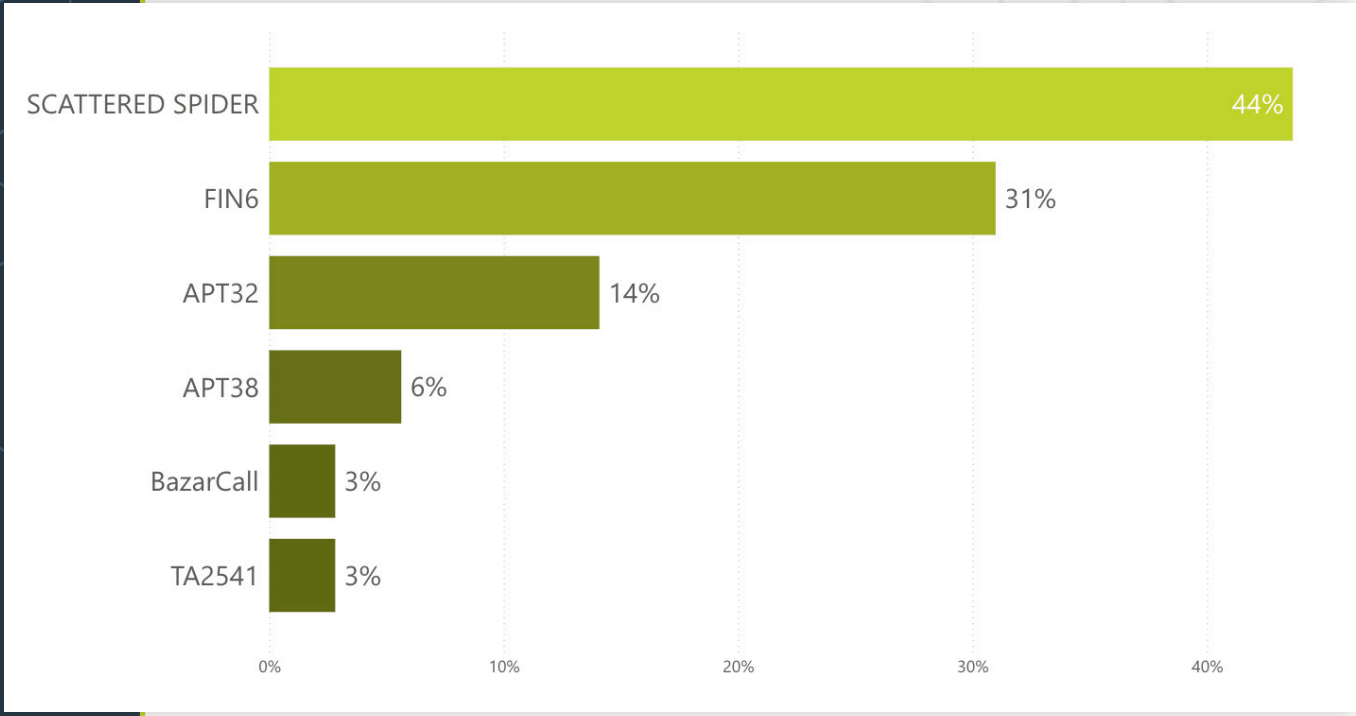


Significant changes between 2022 and 2023 for malware reporting in MISP were:

- Agent Tesla reporting increased slightly from 23% to 27%
- QakBot reporting increased from 6% to 15%
- IcedID reporting doubled from to 5% to 10%
- Remcos reporting dropped drastically from 43% to 4%

Threat Actors & Intrusion Sets

The following graph demonstrates the most common threat actors and intrusion sets (defined as ATT&CK Group) reported by members:

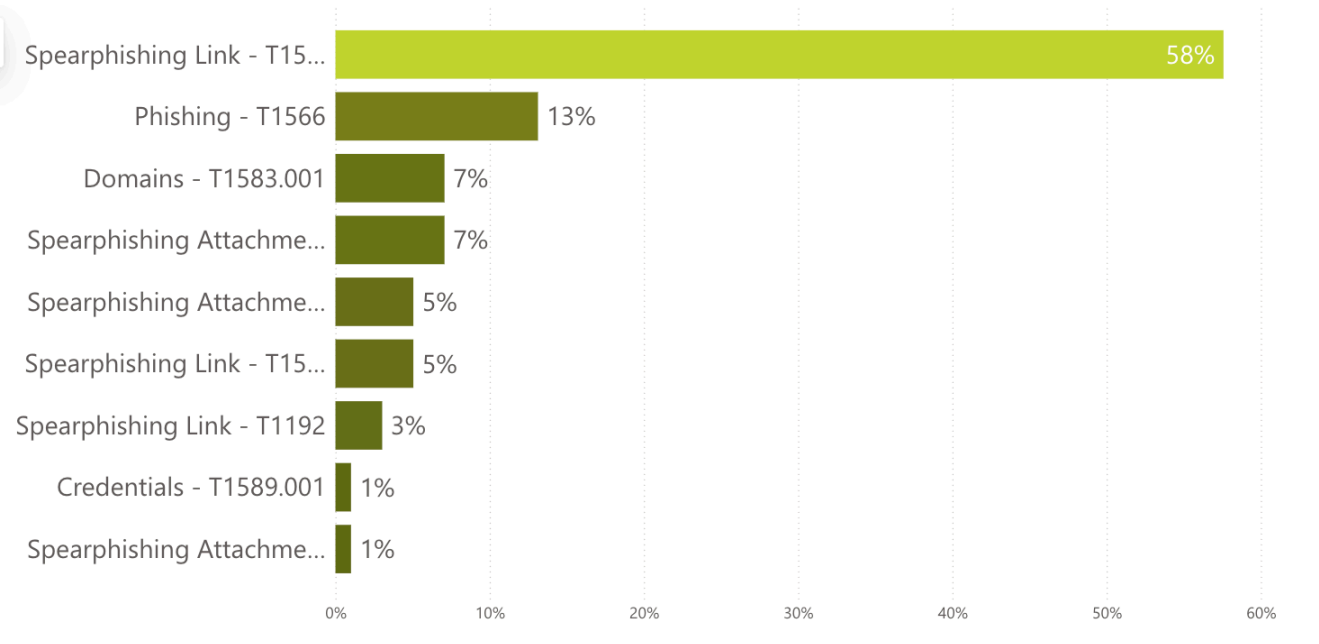


Significant changes between 2022 and 2023 for threat actor and intrusion set reporting in MISP were:

- Scattered Spider was not reported in 2022, and in 2023, made up 40% of attributed threat intelligence
- FIN7 reporting decreased from 31% to 28%
- FIN6 reporting decreased from 31% to 28%
- APT32 reporting decreased from 14% To 13%

TTPs

The following graphs demonstrate the most common MITRE ATT&CK Techniques reported by members:

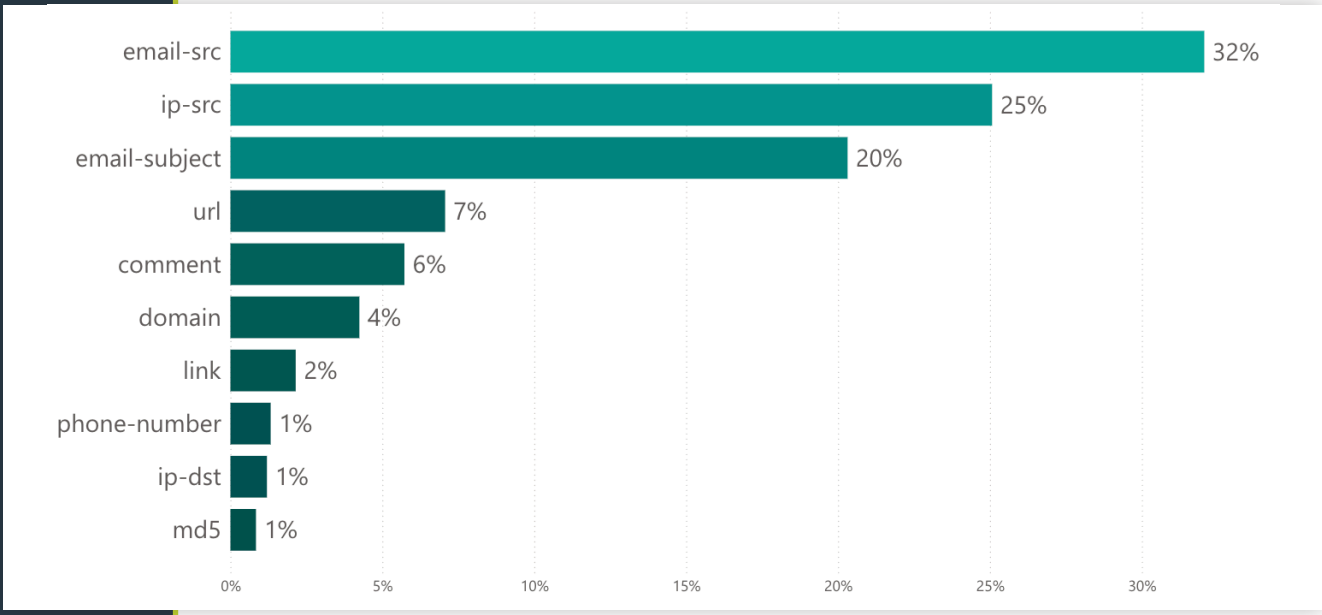


Significant changes between 2022 and 2023 for malware reporting in MISP were:

- Agent Tesla reporting increased slightly from 23% to 27%
- QakBot reporting increased from 6% to 15%
- IcedID reporting doubled from to 5% to 10%
- Remcos reporting dropped drastically from 43% to 4%

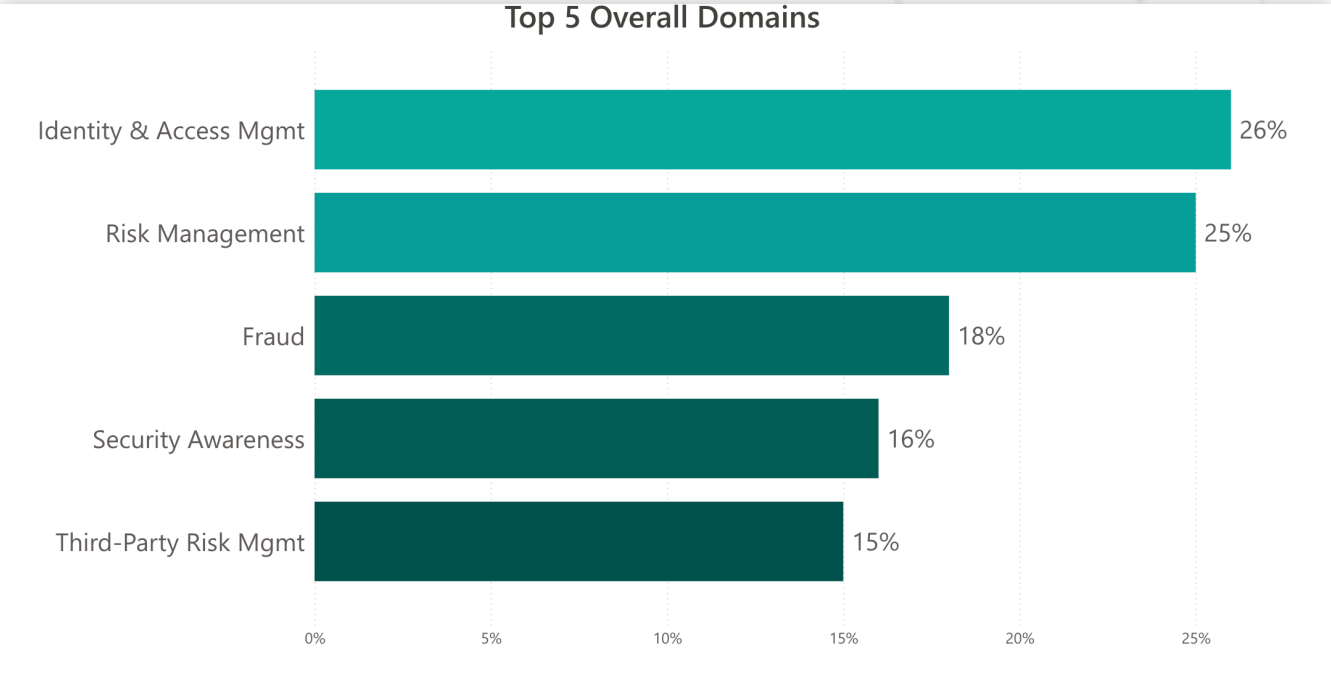
Top Attributes

The following graph demonstrates the most common attribute (indicator of compromise) types reported by members:



Requests for Information (RFIs)

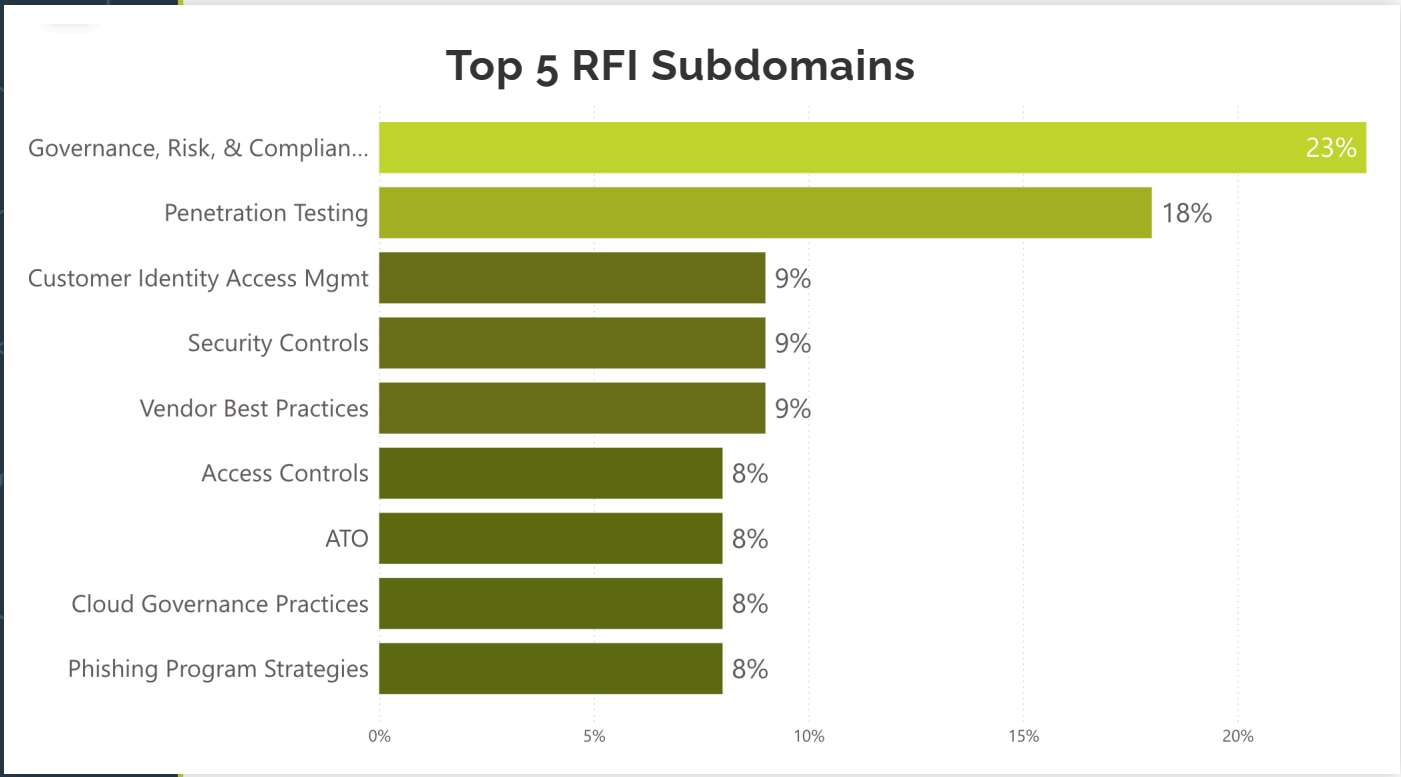
Requests for Information (RFIs) were broken down by domain:



Domain Comparison

For comparison, the key changes in RFI domains between 2022 and 2023 were:

- Identity and Access Management did not make the list for 2022 and in 2023, accounted for 26% of all RFIs, making it the most prevalent domain
- Fraud did not make the list for 2022 and accounted for 18% in 2023, the third most prevalent domain
- Risk Management RFIs decreased from 30% to 25%
- Security Awareness (16%) and Third Party Risk Management (15%) made the list for 2023, while Threat Intelligence (6%), Resilience (14%), Security Operations (14%), and Security Architecture (36%) all fell off the list from 2022

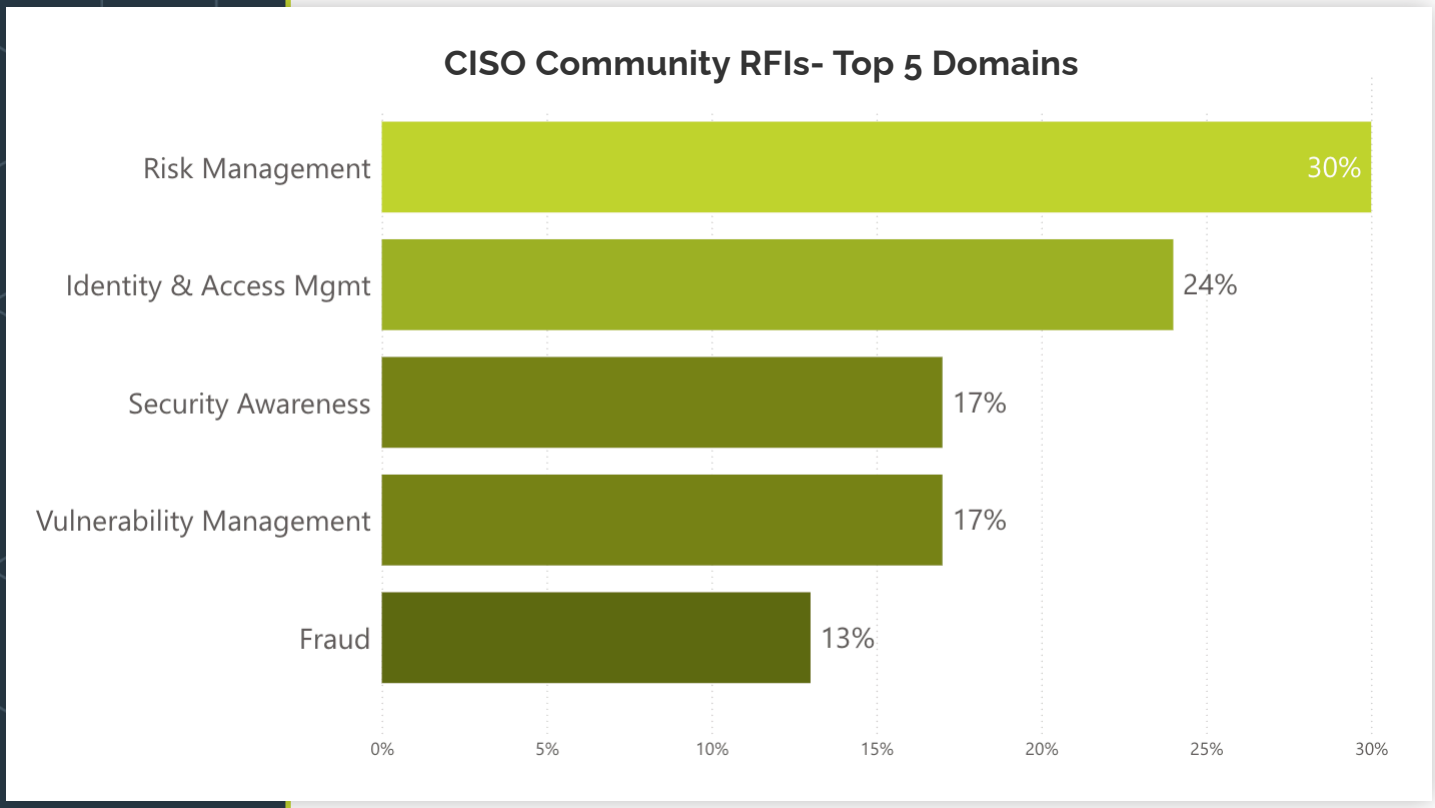


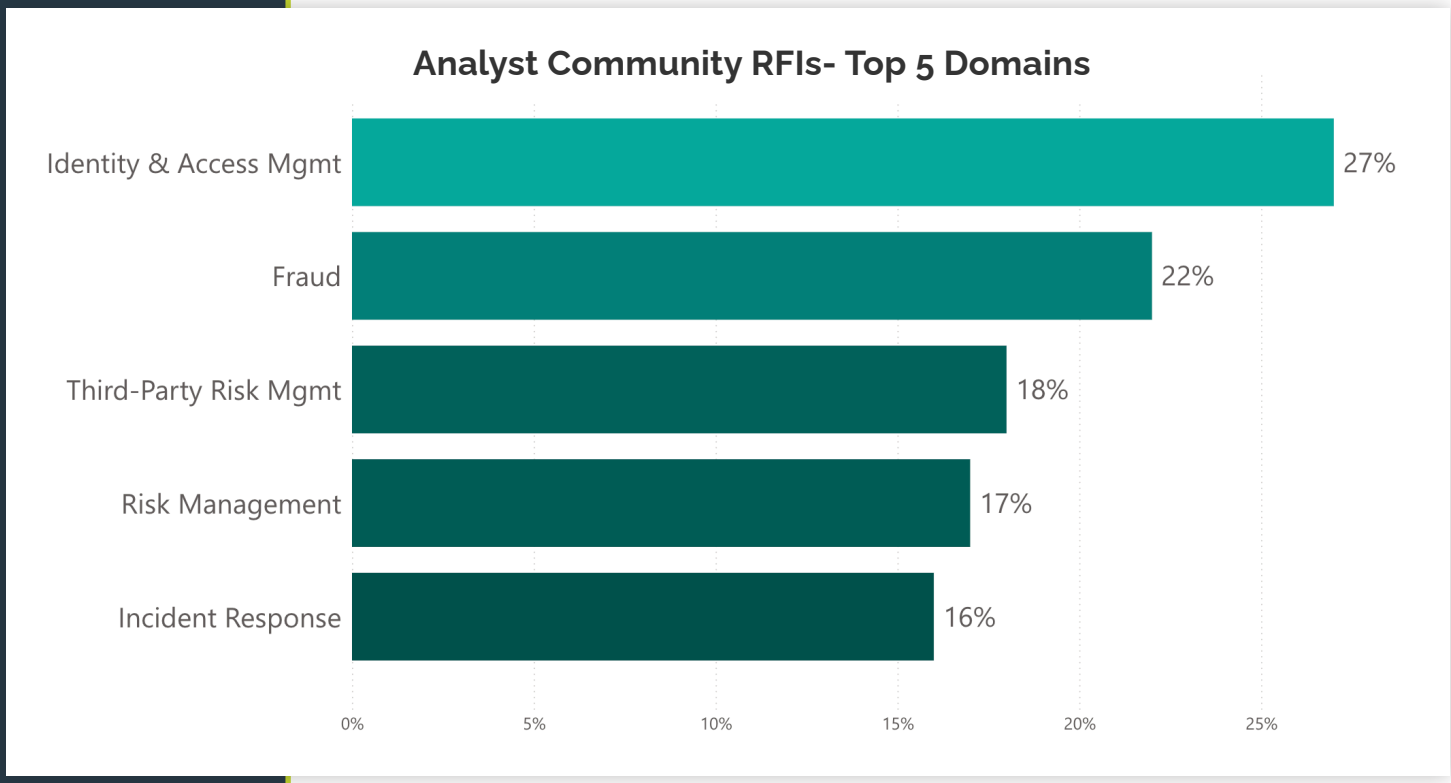
For comparison, in 2022, the top five subdomains were:

- IAM (20%)
- Frameworks and Standards (11%)
- Security Engineering (11%)
- Fraud (7)
- Security Awareness (6%)

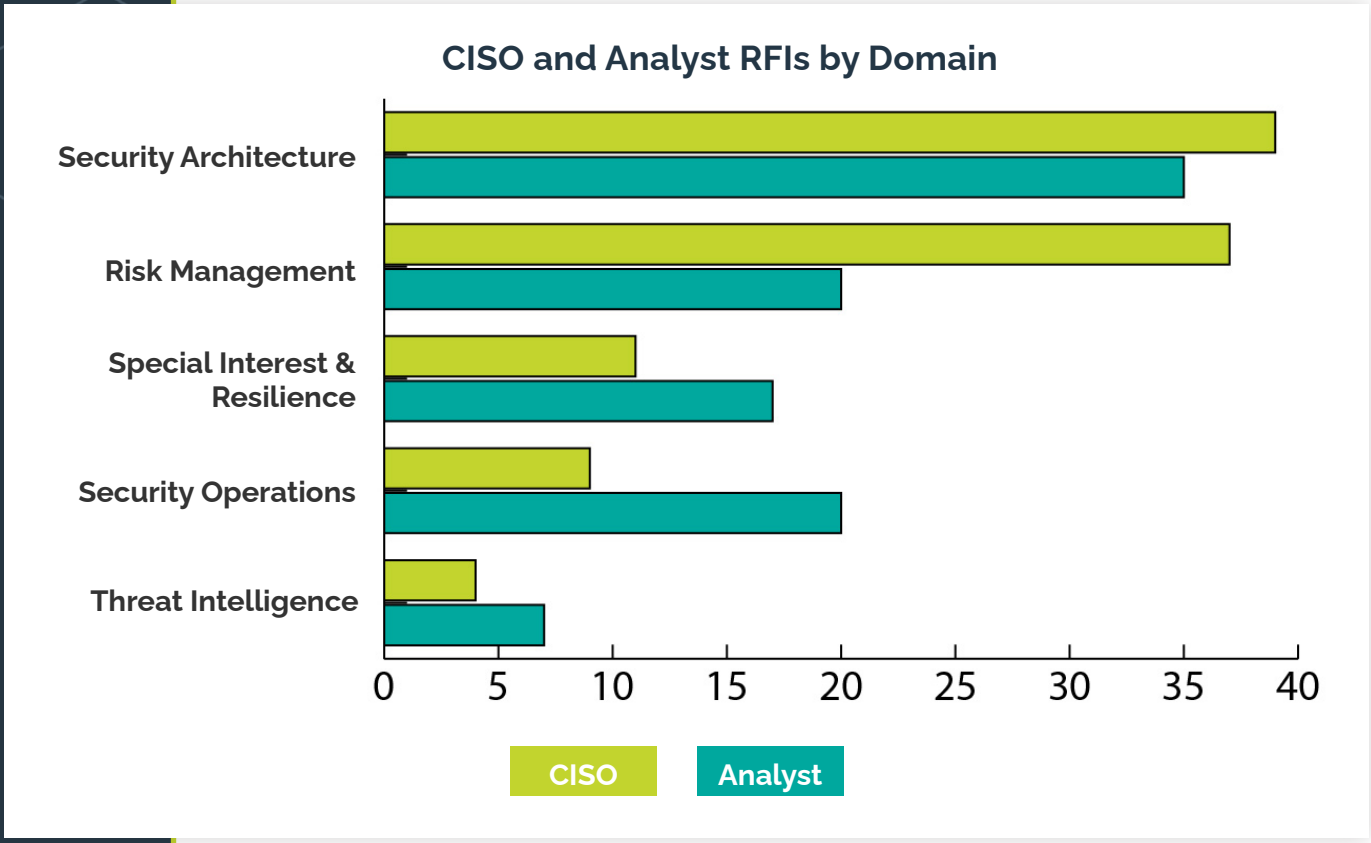
IAM, engineering, fraud, and awareness all appear in subdomain listings rather than domain listings due to improvements in tools and processes used to track community engagement by the RH-ISAC Research and Analytic teams.

RFI Topics by Community





For comparison, top RFI topics by community in 2022 are demonstrated in the graph below:



Surveys Overview

In 2023, RH-ISAC conducted three benchmarks and seven surveys:

CISO Benchmark Report

With a 35% increase in participation in 2023, we learned from 126 companies that a typical RH-ISAC member has 6-8% of their IT budget and 15-25 FTEs dedicated to information security operations. Ransomware, data loss, and cloud security were cited as the top three risks organizations faced.

Practitioner Benchmark Report

According to 105 practitioners surveyed, 83% serve more than one job function and have a diverse skillset across security operations, threat intelligence, and risk management duties; with 63% assessing their skills between intermediate and advanced levels.

Tools & Technology Benchmark Report

One hundred member companies participated in the second annual Tools & Technology Report highlighting the most common tools used by members, including TIP, SIEM, SOAR, XDR, and other solutions.

Survey Reports

The RH-ISAC published seven survey reports on the following topics: Cyber Insurance Premiums, Phishing Programs, Configuration Management Database, Business Continuity & Disaster Recovery, Bring-Your-Own-Device (BYOD) Security, BYOD Stipend Model for Mobile Users, and Fleet Card Security at Fuel Retail Locations.

About RH-ISAC

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cybersecurity information and intelligence. The RH-ISAC connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for consumer-facing industries through collaboration. RH-ISAC serves businesses including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies. For more information, visit www.rhisac.org.