TLP: CLEAR

RETAIL & HOSPITALITY INDUSTRY INSIGHTS

2023 Verizon Data Breach Investigation Report Analysis

RETAIL & HOSPITALITY ISAC

Introduction

With more than 242 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: web application attacks, 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. We also found that for requests for information (RFIs), the community tended to be more interested in policy and organizational issues than threat intelligence, demonstrating the various levels of cybersecurity areas the community manages.

Executive Summary

As in 2022, RH-ISAC analysts reviewed the 2023 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 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: 2023 Verizon DBIR

Key Findings

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

- The most common attack methods were: stolen credentials, phishing, and vulnerability exploits
- The most commonly targeted data were: personally identifiable information (PII), credentials, and internal data
- 91% of industries saw ransomware in the top three most prevalent threats
- Ransomware held steady at 24% of breaches
- 50% of social engineering attempts involved pretexting: the fabrication of scenarios to pressure victims into divulging sensitive information
- 83% of breaches originated from external actors
- 95% of breaches were financially motivated
- Log4j was a major concern for cyber defenders across multiple industries, with 90% of vulnerability exploit incidents referencing Log4j
- The most prevalent threat actor type was organized crime
- Key MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) included 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:

- Business Email Compromise (BEC) attacks nearly doubled, representing over 50% of social engineering incidents
- Payment data dropped significantly down the list of heavily-targeted data types
- The prevalence of Log4j related incidents and scans, especially in the first half of 2022

Key Industries

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

- Accommodation rose five places from 17th most targeted industry in 2021 to 12th for 2022
- Retail fell one place from 9th to 10th
- Wholesale rose one place from 16th to 15th
- Transportation fell one place from 10th to 11th
- Manufacturing rose one place from 6th to 5th
- Entertainment rose four places from 13th to 9th

Metrics & Trends by Industry

Core metrics and trends from the Verizon report for industry categories that most closely align with hospitality members of the RH-ISAC community are as follows:

	Incidents & Breaches	% of Breaches Executed by External Actors	% of Attacks Financially Motivated	Primary Targeted Data	Notable Trends
Retail	**406 Incidents** *(down from 629 in 2021)* **193 Confirmed Breaches** *(down from 241 in 2021)*	94%	100%	Credentials PII Payment Data	System intrusion, social engineering, and basic web application attacks made up 88% of breaches Magecart style attacks represent about 18% of breaches
Accommodation	**254 Incidents** *(up from 156 in 2021)* **68 Confirmed Breaches** *(down from 69 in 2021)*	93%	100%	Payment Data Credentials PII	Similar to Retail, system intrusion; social engineering; and basic web application attacks made up 90% of breaches Notably, Verizon reported a complete drop off in espionage-motivated attacks, down from 9% in 2021
Manufacturing	**1,817 Incidents** *(down from 2,337 in 2021)* **263 Confirmed Breaches** *(down from 338 in 2021)*	90%	96%	PII Credentials	Like Retail and Hospitality, system intrusion; social engineering; and basic web application attacks made up 83% of breaches Denial of Service (DoS) attacks made up roughly 67% of incidents

Metrics & Trends by Geography

Verizon also provided key data for several geographic regions:

	Incidents & Breaches	% of Breaches Executed by External Actors	% of Attacks Financially Motivated	Primary Targeted Data	Notable Trends
Asia-Pacific	699 Incidents 164 Confirmed Breaches	92%	61% (39% espionage motivated)	Internal Data Trade Secrets Credentials	System intrusion; social engineering; and basic web application attacks made up 93% of breaches
Europe, Middle East, and Africa	2,557 Incidents 637 Confirmed Breaches	98%	91%	Credentials Internal Data System Data	System intrusion; social engineering; and basic web application attacks made up 97% of breaches
Latin America	535 Incidents 637 Confirmed Breaches	95%	91%	System Data Internal Data Classified Data	System intrusion; social engineering; and basic web application attacks made up 97% of breaches
North America	9,036 Incidents 65 Confirmed Breaches	94%	91%	System Data Internal Data Classified Data	System intrusion; social engineering; and basic web application attacks made up 85% of breaches

Metrics & Trends for Small & Medium Sized Businesses

Verizon provided the following key metrics for small (less than 1,000 employees) and medium (more than 1,000 employees) sized businesses:

	Incidents & Breaches	% of Attacks Financially Motivated	Primary Targeted Data	Notable Trends
Small Businesses	699 Incidents 381 Confirmed Breaches	94%	Internal Data Credentials System Data	System intrusion; social engineering; and basic web application attacks made up 92% of breaches
Medium Businesses	496 Incidents 227 Confirmed Breaches	97%	Internal Data Credentials System Data	System intrusion; social engineering; and basic web application attacks made up 85% of breaches

Verizon also recommended that less mature security organizations focus on three key controls from the CIS Critical Security Control Navigator for the most effective defense with limited resources:

- Security Awareness and Skills Training
- Data Recovery
- Access Control Management

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 were key top threats reported and discussed in the RH-ISAC community, which aligns with top threats in the Verizon DBIR.

DoS Attacks

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.

BEC Attacks

Member discussion of BEC attacks on sharing platforms increased over 2022, corresponding to the massive increases noted by Verizon.

Log4j

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.

Customer Payment Data

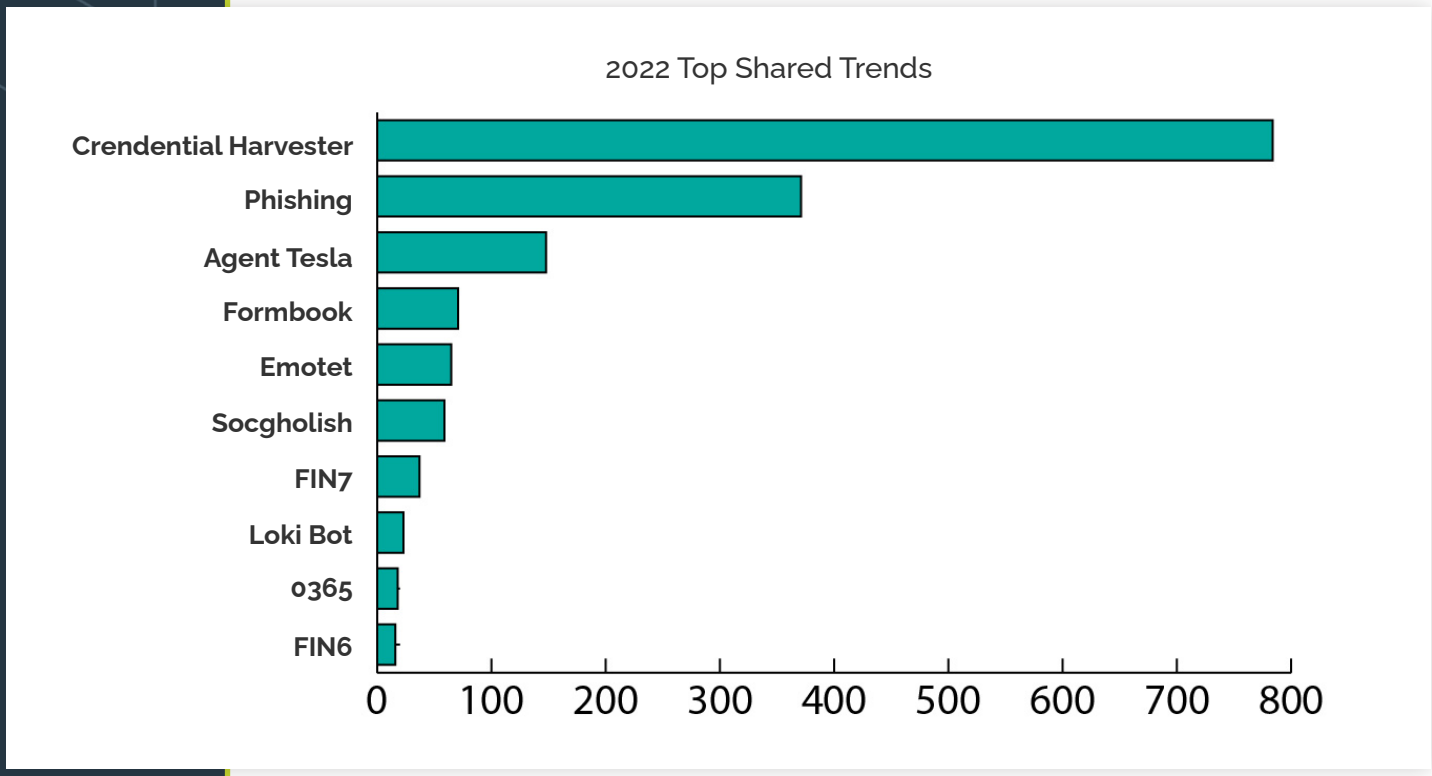
Attacks targeting customer payment data are among the top concerns for RH-ISAC members, which aligns with the granular view of industry-specific metrics provided by Verizon.

2022 Top Sharing Trends

Th graph below illustrates the RH-ISAC community's shared threat trends for 2022, which can be described as the frequency that threats were shared through Member Exchange, Slack, and the Core Member Listserv.

For 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 the most prominent threats facing organizations in the retail, hospitality, and travel sectors. Phishing and credential-stealing threats are both 1) greater focus areas and 2) quantitatively more prevalent active threats than other prominent threats.

TOP MISP SHARING THEMES in 2022

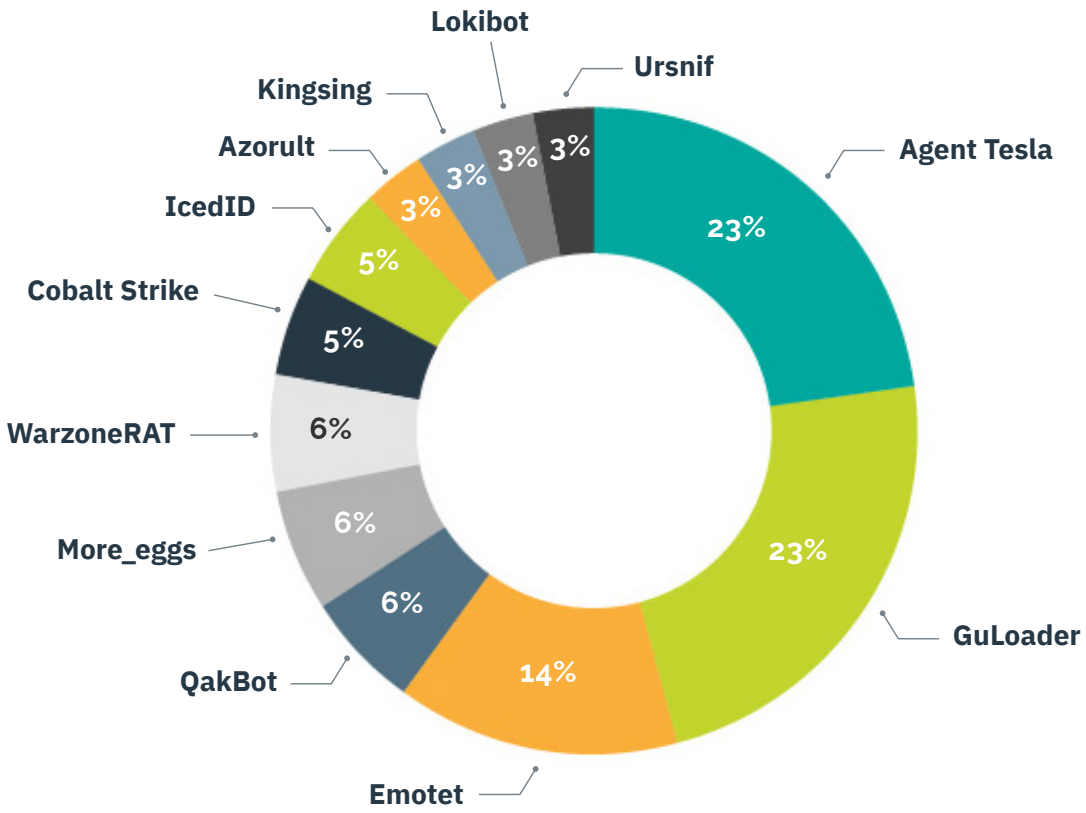
Throughout the second half of 2022 and the first half of 2023, the RH-ISAC intelligence team worked actively on developing sharing and tracking capabilities for technical intelligence from the membership community. These enhancements to MISP allow the RH-ISAC community to track technical intelligence at a granular level, and to conduct in depth relationships by pivoting on additional context from enriched intelligence.

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:

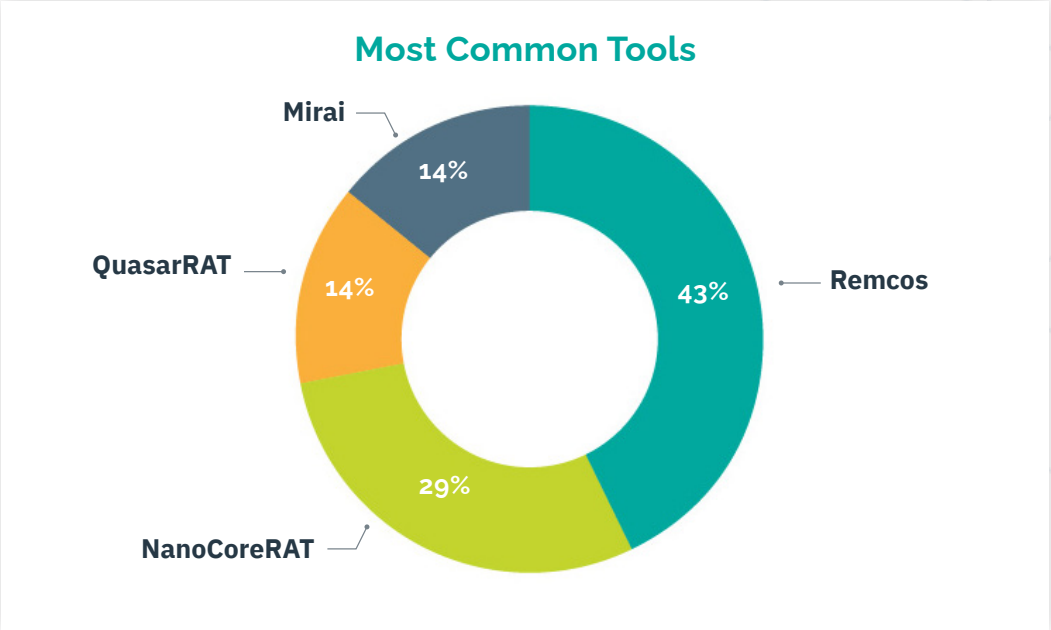
Malware and Tools

The following graphs demonstrate the most common malware (defined as ATT&CK Software) reported by members:

Most Common Malware

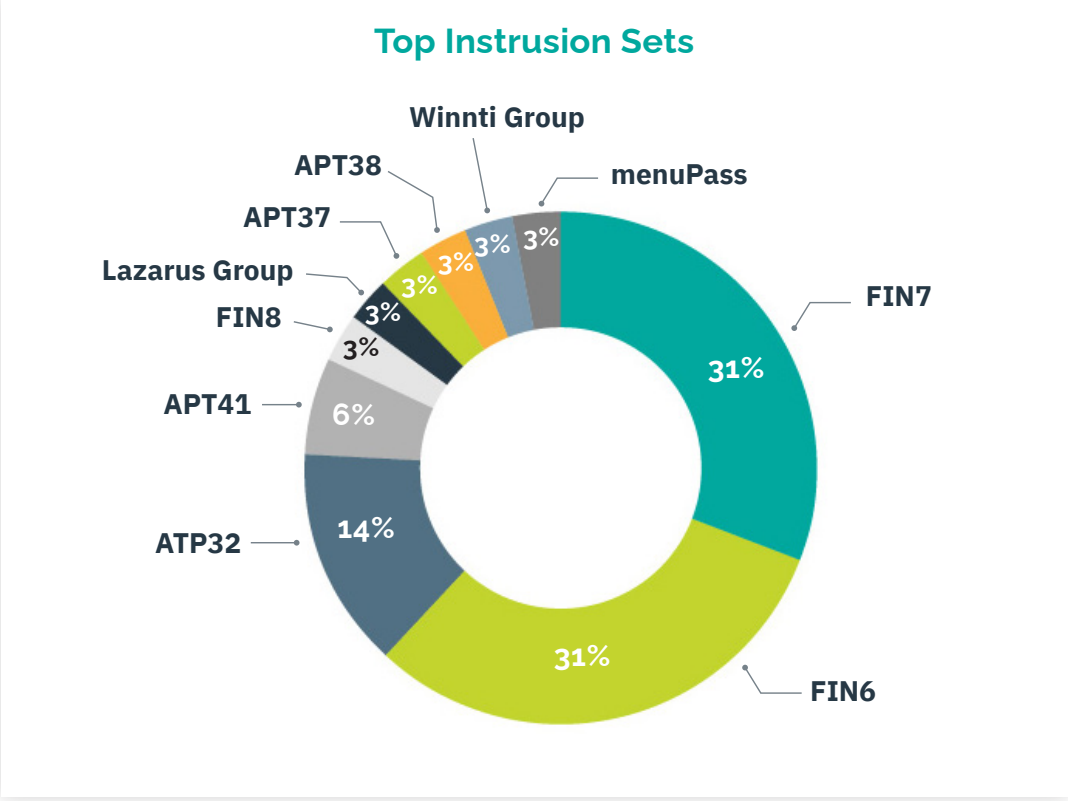


The following graphs demonstrate the most common tools (defined as ATT&CK Software, used in the delivery of additional malware) reported by members:

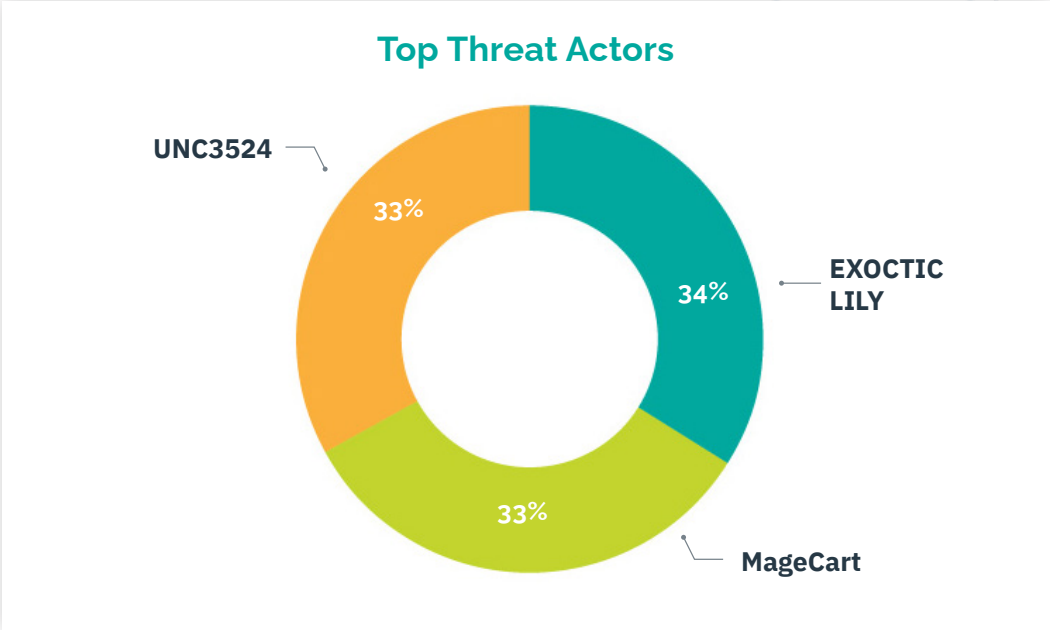


Intrusion Sets and Threat Actors

The following graphs demonstrate the most common intrusion sets (defined as ATT&CK Group) reported by members:

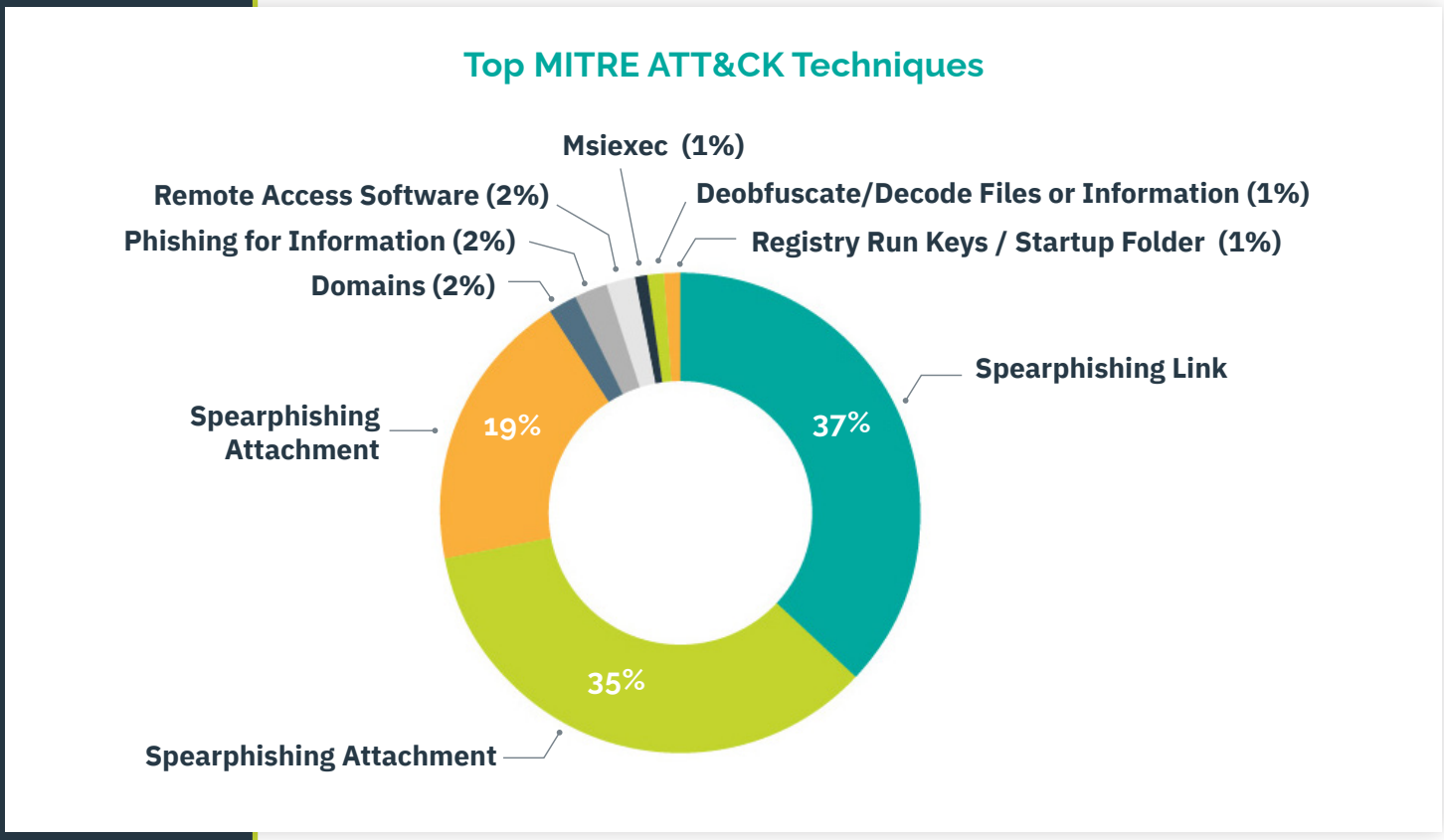


The following graphs demonstrate the most common threat actors (defined as characteristics of malicious actors or adversaries representing a cyberattack threat including presumed intent and historically observed behavior) reported by members:



TTPs

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



Top Shared RFIs

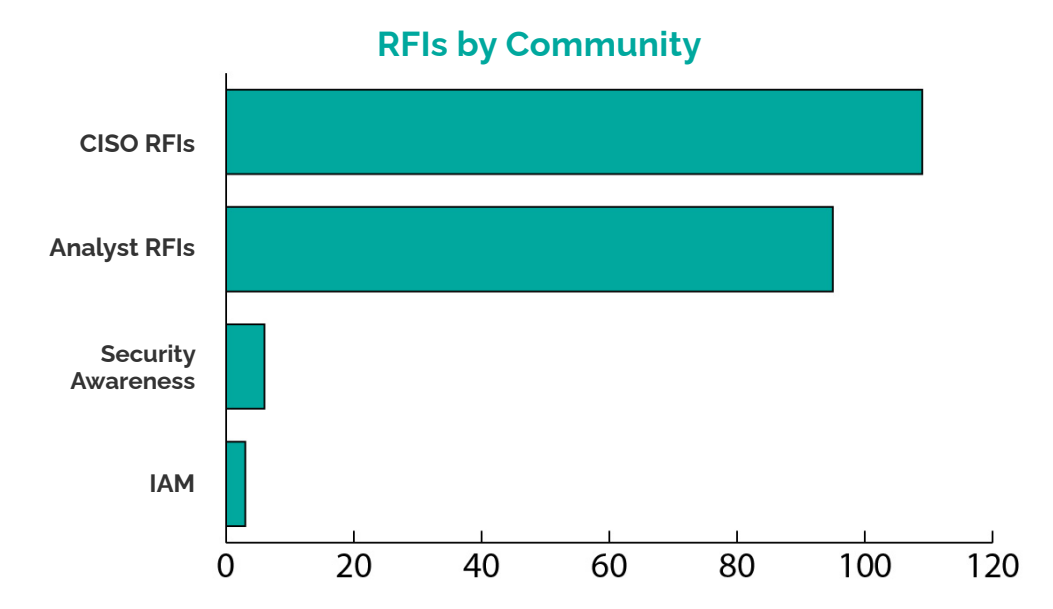
Theme	Total Shares
Cyber Awareness Solutions	23
WFH Performance Monitoring	18
Business Issues Related to the Expeditors International Cyber Incident	17
Data Retention	16
Job Candidate Scams	16
Legal Disclaimer to Bounty Hunters	15
Threat Intel Platform (IOCs Only)	15

Key changes from 2021 RFI trends include:

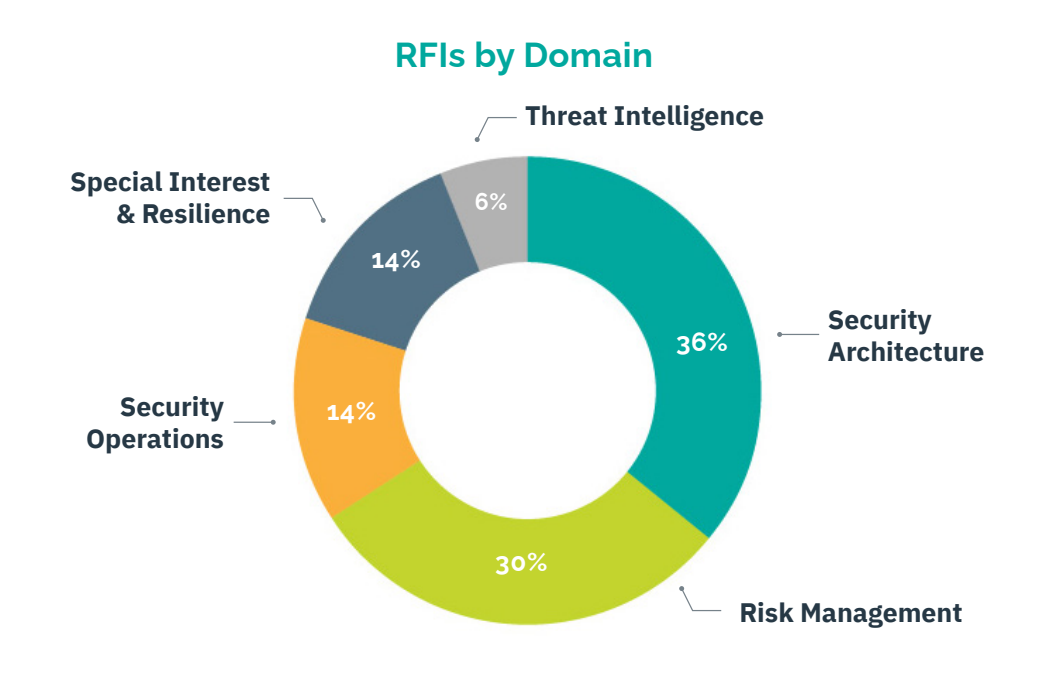
- In 2021, most shared Requests for Information (RFIs) and responses in the RH-ISAC community were policy or organizationally related, rather than focused on threat intelligence or recent cyberattacks. In 2022, the top RFIs and responses focus on a mix of policy and threat intelligence topics
- The top topic for RFIs in 2022 was vendors that provide phishing simulation campaigns and conduct cyber awareness training efficiently and effectively
- Only one topic appears on the list of most active RFIs and responses for both 2021 and 2022: work from home policy, which fell from 1st place with 32 shares to 2nd place with 18 shares
- RFI topics for both Cyber awareness emerged as the top concern at 23 shares, after not making the list in 2021

RFI Breakdown

In 2022, RH-ISAC received 213 RFIs which marks a 21% increase compared to the previous year. These RFIs came through the Analyst, CISO, IAM, and Security Awareness Communities on Member Exchange. The Analyst community was most active in soliciting information, followed closely by the CISO community. The breakdown of RFIs community-wise was as follows:



RFIs received were further broken down by domain. Similar to 2021, Security Architecture continued to be of primary interest to the overall community in 2022, followed by Risk Management, Security Operations, Special Interest and Resilience, and Threat Intelligence.



Breakdown of Domain and Subdomain Interests

Security Architecture

- 55% - Identity & Access Management
- 31% - Security Engineering (Tool Integrations & Use Cases)
- 14% - others, including Application and Software Development, Digital Transformation & Cloud Security, Operational Technology & Internet of Things (IoT), Tools and Technologies (Use Cases) and Security Awareness

Risk Management

- 37% - Frameworks & Standards
- 17% - Security Awareness
- 16% - Third-Party Risk Management
- 14% - Governance & Compliance
- 16% - others, including Executive Reports and Scorecards, Insider Threat and Risk Assessment

Security Operations

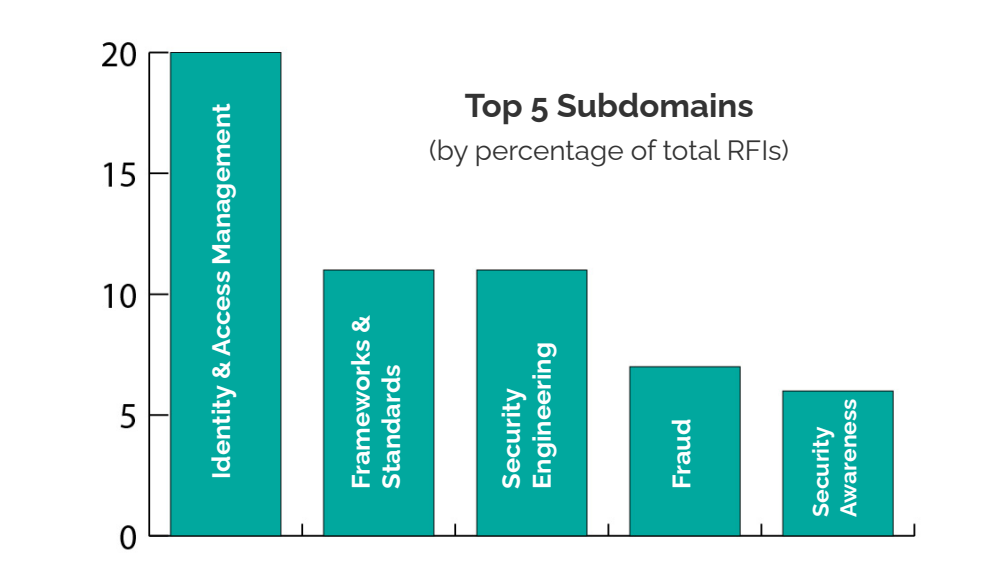
- 32% - MSSP & Outsourced Security Services
- 29% - Incident Response
- 23% - Vulnerability Management
- 16% - others, including Penetration Testing and SOC Operations

Special Interest and Resilience

- 52% - Fraud includes RFIs such as job candidate scams, gift cards, and loyalty points fraud
- 21% - ATO
- 14% - Industry Collaboration
- 13% - others, including Ransomware and Social Engineering

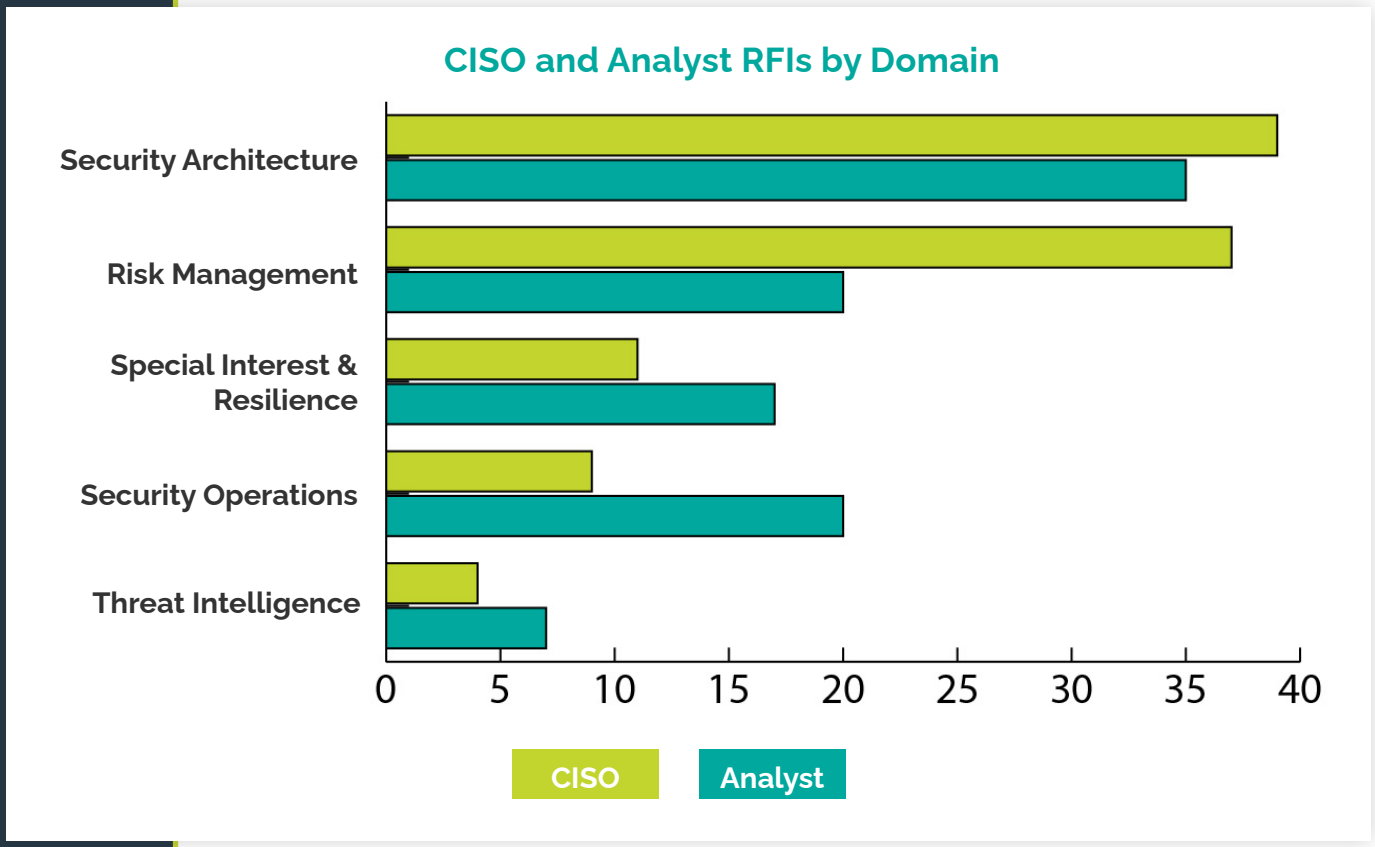
Threat Intelligence

- 38% - Threat Actor Profiles and TTPs
- 31% - Tradecraft
- 23% - Sources and Feeds include RFIs such as threat intelligence programs, detecting data leaks, and engaging with customers who received phishing emails.
- 8% - Darkweb



RFI Topics by Community

The CISO community's greater interests were Security Architecture, Risk Management, and Special Interest and Resilience, respectively. In contrast, the Analyst community's interest focused on Security Architecture, followed by Risk Management and Security Operations. The CISO Community saw a total of 95 RFIs, and the Analyst Community saw a total of 109.



Surveys Overview

In 2022, RH-ISAC conducted five surveys:

Vulnerability Management

In June 2022, The Research & Education team surveyed the CISO community to understand how organizations manage vulnerabilities (VM), prioritize, and report risk.

Underage Pornography Checks

In July 2022, a member posted a Request for Information (RFI) in the Analyst Community seeking advice on how to check files downloaded by employees from pornography sites to ensure they do not contain underage pornography. The member also requested a survey to determine if other organizations review each image and video to ensure compliance.

Alfahive Cyber Risk Quantification

In August 2022, RH-ISAC partnered with Alfahive, an associate member specializing in cyber risk quantification, to conduct a survey that measures how relevant risk is to different parts of the organization: online sales, store sales, supply chain, HR & finance, and IT & software infrastructure.

FIDO Assessment for Passwordless Authentication

In August 2022, RH-ISAC surveyed its members to gauge their familiarity and interest in the FIDO standard for passwordless authentication.

Cyber Insurance Premium Survey

In September 2022, the RH-ISAC distributed a survey to the CISO Community to better understand cyber insurance coverage and premium costs.

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.