TLP: WHITE

RETAIL & HOSPITALITY INDUSTRY INSIGHTS

2022 Verizon Data Breach Investigation Report Analysis

RETAIL & HOSPITALITY ISAC

Introduction

With more than 200 member companies from the retail and hospitality industry, the threat intelligence shared by our RH-ISAC membership is an excellent representation of the trends impacting our sector, but 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, manufacturing, and entertainment sectors faced many of the same threats that our members reported: web application attacks, credential stealing, ransomware, and phishing, originating from external threats, 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 detail for the community threat landscape, such as specific malware targeting members. We also found that for RFIs, the community tended to be more interested in policy and organizational issues than threat intelligence, demonstrating the various levels of cybersecurity the community manages.

KEY TAKEAWAYS: Verizon DBIR

Trends & Findings

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.

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

- The most common attack methods were: stolen credentials, ransomware, and phishing
- The most commonly targeted data were: payment data, personally identifiable information (PII), credentials, intellectual property, and non-sensitive data
- 73% of breaches were executed by external actors, and 18% of breaches were executed by internal actors
- 39% of attacks originated with third-party vendors
- 82% of incidents resulted from human error, and these errors were split between clicking on phish links and failing to follow standards which resulted in business email compromise.
- Most indicators of compromise (IOCs) had relatively good value for blocking
- Hashes had relatively low value, but IP addresses, domains, network artifacts, tools, and TTPS all were valuable for blocking

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:

	# of Data Breaches	% of Breaches Executed by External Actors	# of Total Incidents	Primary Targeted Data	% of Attacks Financially Motivated	Notable Trends
Retail	241	87%	629	Credentials PII Payment Data	98%	Instances of attacks using malware to enumerate the capture of application data were 7 times higher for retail organizations than in other industries. Capturing application data is common in attacks where threat actors dwell in e-commerce servers to steal payment data over time. Retail organizations most commonly learn of breaches via fraud detection methods.
Accommodation and Food Services	69	90%	156	Credentials PII Payment Data	91%	Attacks against this sector have dramatically decreased since 2012 from over 54% of all cases to less than 2% of cases
Manufacturing**	338	88%	2,337	Credentials PII Payment Data	88%	In 2016: 55% of attacks on manufacturing were cyberespionage attacks seeking proprietary data. In 2021: 88% of attacks were financially focused seeking payment data
Arts, Entertainment, and Recreation*	96	74%	215	Credentials PII Medical Data	91%	This industry has a higher percentage of insider threats (26%) than other industries. Denial of Service (DoS) attacks are notably common in this sector, especially among gaming organizations in the Asia-Pacific (APAC) region

*** Manufacturing is closely tied to the RH-ISAC sectors' critical functions so it is included in this report*

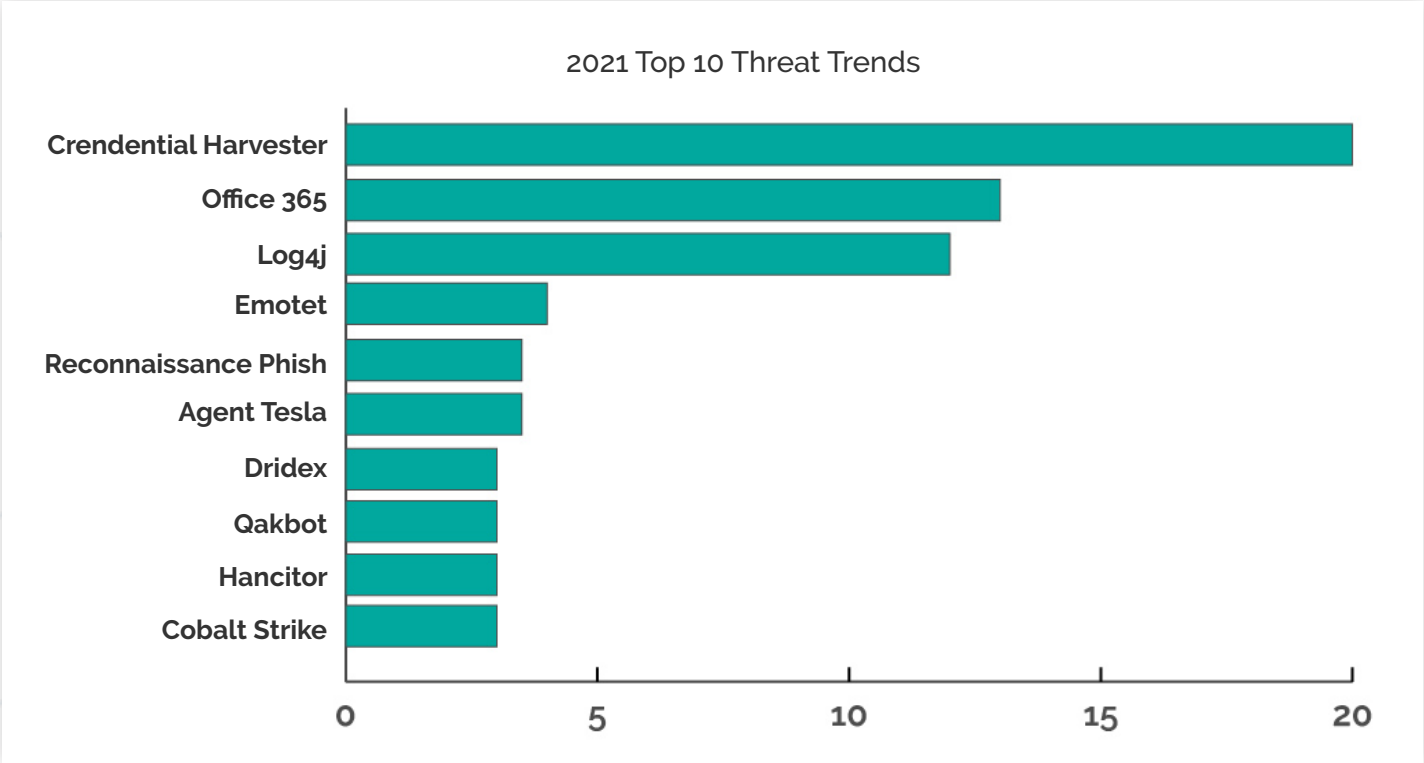
** This sector includes gaming organizations and is thus included here for the RH-ISAC members whose operations include gaming*

KEY TAKEAWAYS: RH-ISAC

2021 Top Attack Trends

The graph below shows the total volume of threat indicators shared related to a given topic. For 2021, RH-ISAC members reported a total 28,344 individual instances of malware. Of these reported instances:

- 20%, or 5,604 instances, were for credential harvesting
- 13%, or 3,602 instances, were for Office-365
- 12%, of 3,374 instances, were for Log4J
- The remaining top seven threat indicator trends, each at 4% (or approximately 1,200 instances) or lower, were split between Emotet, other phishing attempts, Agent Tesla, Dridex, Qakbot, Hancitor, and Cobalt Strike



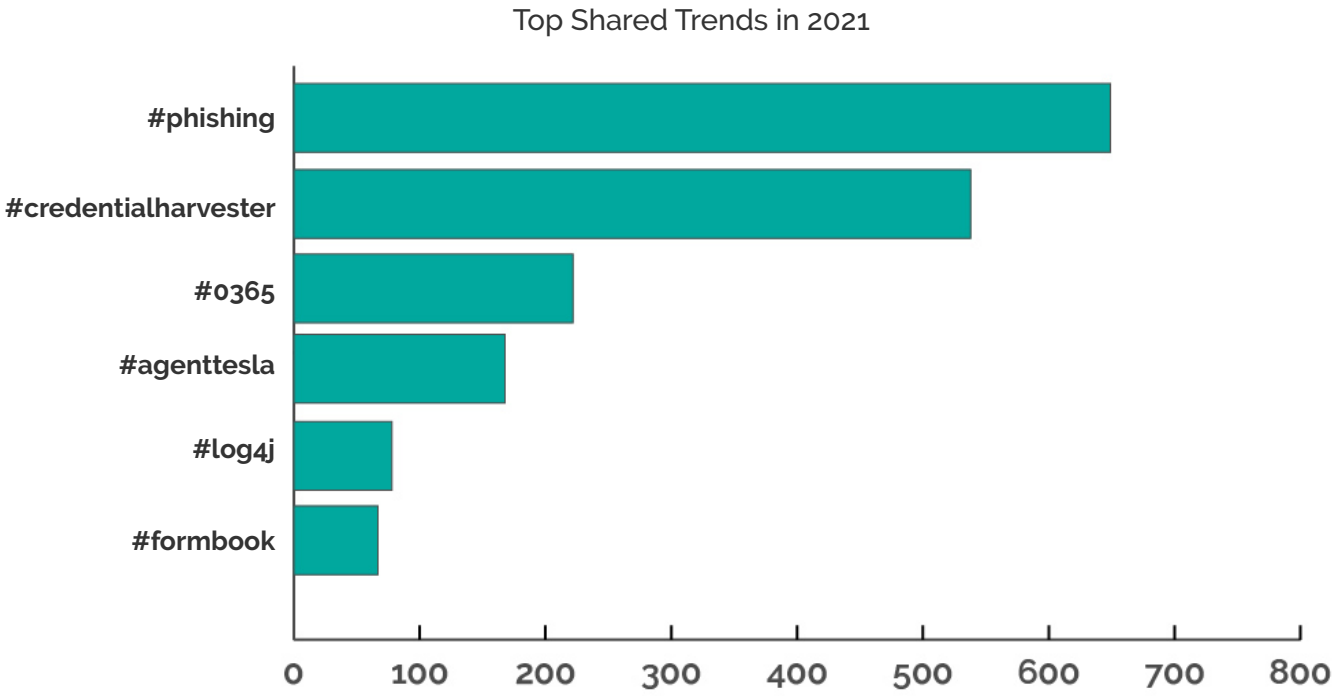
While the Verizon report did not specify the individual malware most prevalent in their research, their placement of credential theft as the primary threat to the retail, accommodation, and arts and entertainment sectors matches up with RH-ISAC data. According to our tracking, credential harvesting represented a significantly more prevalent threat to membership than the remaining top nine threats.

Verizon reported that the majority of incidents they researched focused on using malware to capture payment data or deliver ransomware, which also tracks with RH-ISAC data. Ransomware and phishing attempts make up a significant portion of the top 10 threats reported by members in 2021.

TOP SHARING THEMES in 2021

Threat Intelligence Sharing Trends

The graph below illustrates the RH-ISAC community's shared threat trends for 2021, which can be described as the frequency that threats were shared through Member Exchange, Slack, and the Core Member Listserv.



As with the Top Threat Trends graph on page 5, the Top Shared Trends corroborate Verizon's primary findings that phishing and credential-stealing are the most prominent threats facing organizations in the retail, hospitality, and travel sectors.

Members shared phishing-related intelligence 649 times and credential-stealing intelligence 538 times on RH-ISAC platforms in 2021, which are significantly higher than the sharing rates of the next most common themes, Office 365 (222 shares), Agent Tesla (168 shares), Log4J (78 shares), and FormBook (67 shares). Phishing and credential-stealing threats are both:

1. greater focus areas
2. quantitatively more prevalent active threats than other prominent threats.

RFI THEMES in 2021

Top Shared RFIs

Interestingly, the most shared Requests for Information (RFIs) and responses in the RH-ISAC community for 2021 were policy or organizationally related, rather than focused on threat intelligence or recent cyberattacks.

Theme	Total Shares
RFI - Continued "work from home" post-pandemic	32
RFI - Vulnerability Management Team Size	20
RFI - Budgets	19
RFI - Recommendations for a Tier 1 MSP	18
RFI - Benchmarking and Security Rating Vendors	16
RFI - GRC tools	16
RFI - IR Notification and Call Center Contracts	15
RFI - Holiday Freeze Poll	15

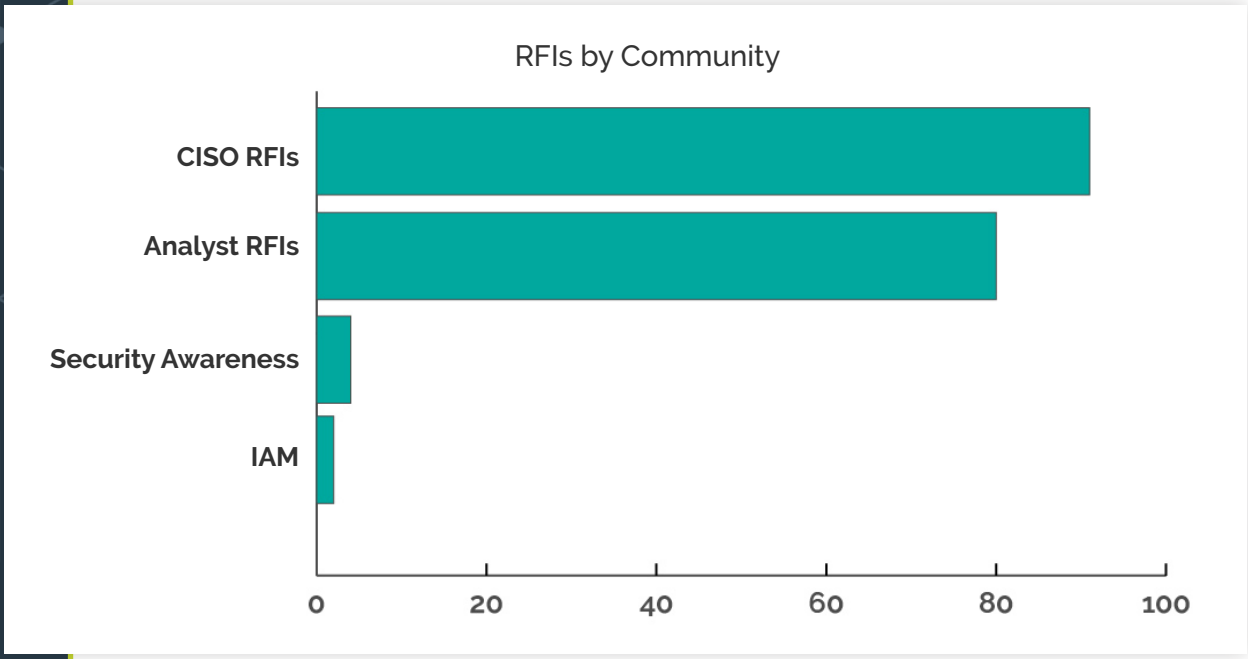
The top issues that RH-ISAC members sought information from peer organizations on in 2021 were matters of critical policy: work from home arrangements after the COVID-19 pandemic, building vulnerability management teams, budgetary priorities, managed service provider recommendations, and vendor assessments topped the list.

In Member Exchange, members asked questions about phishing awareness training, critical vulnerability exploits (CVEs), and common scam tactics. In Slack, the conversation focused more heavily on threat actors and tactical-level malicious activity such as ransomware IOCs, threat actor tactics, techniques, and procedures (TTPs), and fixes for vulnerabilities.

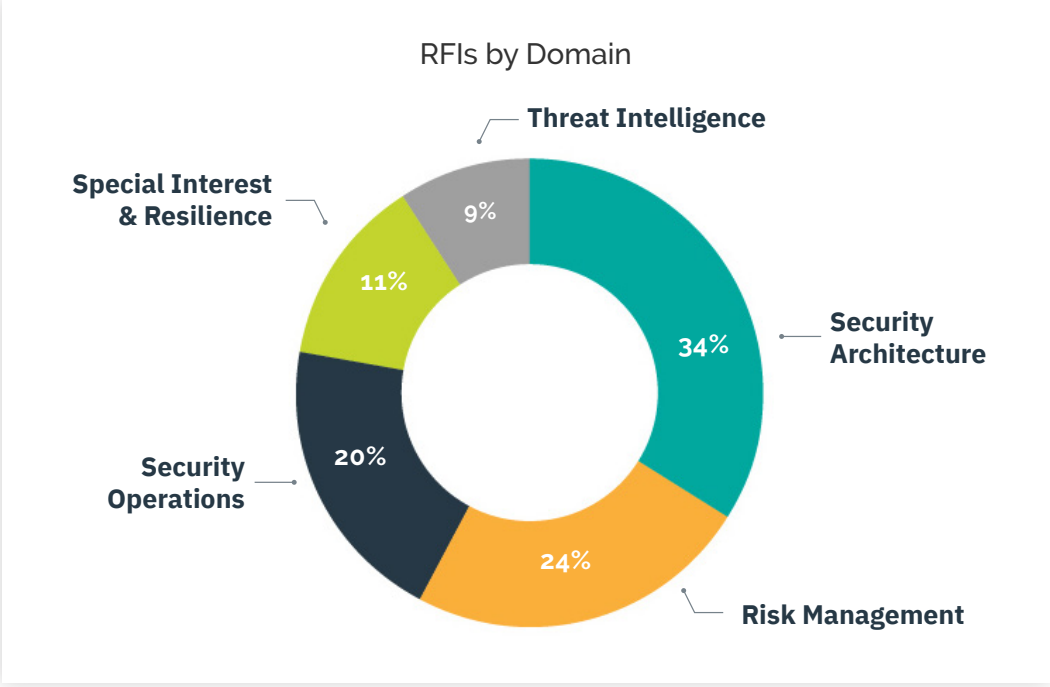
In addition to the threat intelligence focus of the Verizon report, this data from RH-ISAC sharing platforms highlights the complexity and nuance of the cybersecurity challenges facing members, which can often be organizational and structural as much as tactical.

RFI Breakdown

In 2021, RH-ISAC received 176 RFIs, including from the Analyst, CISO, IAM, and Security Awareness Communities. The CISO community was most active in soliciting information, followed closely by the Analyst community. In comparison, the Security Awareness and Identity Access Management (IAM) communities were much less active.



RFIs were also broken down by domain. Security Architecture was the primary interest among the overall community for 2021, followed by Risk Management, Security Operation, Special Interest and Resilience, and Threat Intelligence.



Breakdown of Domain and Subdomain Interests

Security Architecture

- 47% — Identity and Access Management
- 28% — Tools and Technologies (Use Cases)
- 13% — Security Engineering (Tool Integrations and Use Cases)
- 12% — others, including Application and Software Development, Digital Transformation/Cloud Security and Operational Technology, and Internet of Things (IoT)

Risk Management

- 23% — Frameworks and Standards
- 23% — Governance and Compliance
- 12% — Executive Reports and Scorecards
- 12% — Security Awareness
- 12% — Third-Party Risk Management
- 18% — others, including Risk Assessments and Data Loss Prevention

Security Operations

- 34% — MSSP/Outsourced Services
- 20% — Vulnerability Management
- 17% — SOC Operations
- 29% — others, including Penetration Testing and Incident Response, Ransomware, and Dark Web

Special Interest and Resilience

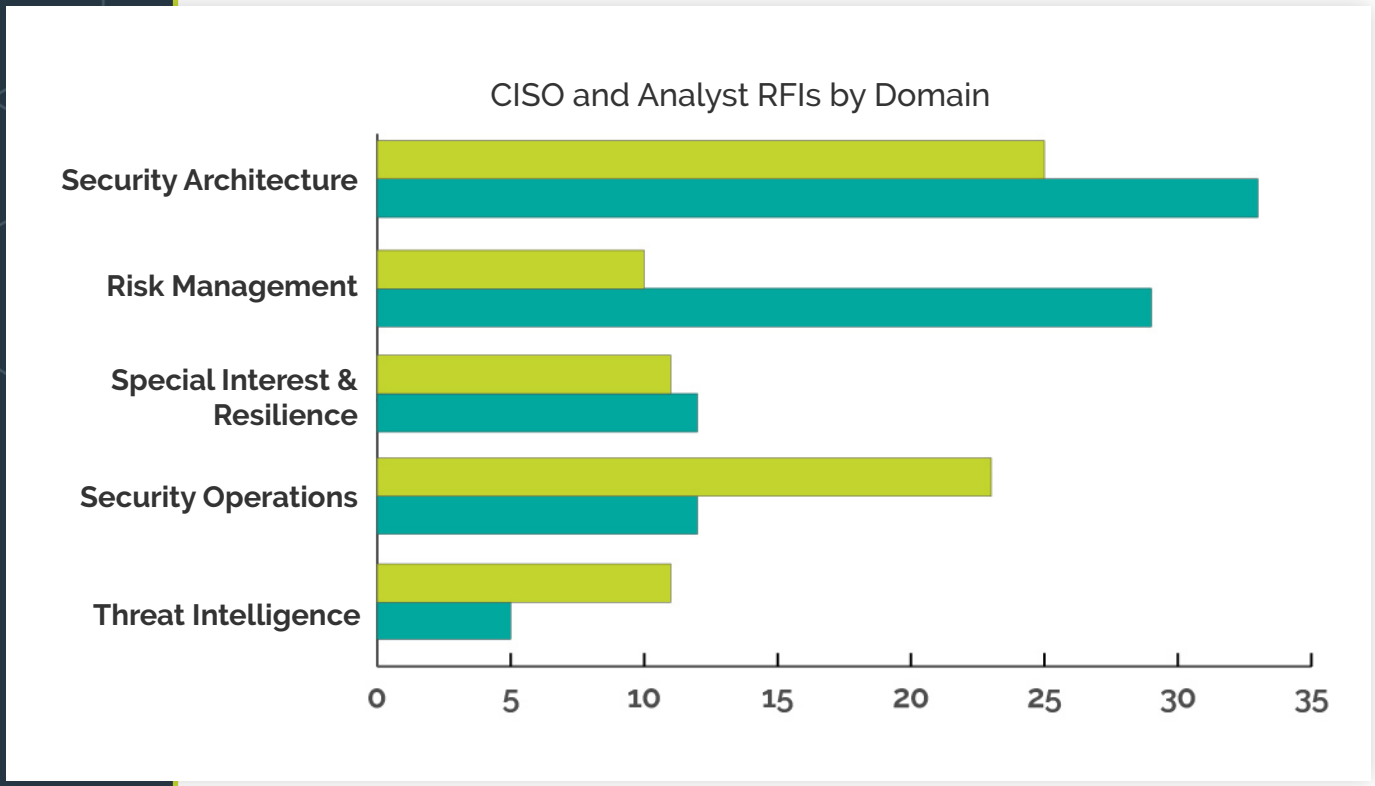
- 34% — Fraud
- 21% — Ransomware
- 45% — others, including Industry Collaboration, Bot Mitigation, and Social Engineering

Threat Intelligence

- 56% — Sources and Feeds, which includes RFIs such as Vishing Scams, Old Malware Detections, etc.
- 31% — Threat Actor Profiles and TTPs
- 13% — others, including Dark web and Splunk discussion

RFI Topics by Community

RFIs received were further broken down into the CISO and Analyst Communities. The CISO community's greater interest lies in Security Architecture, Risk Management, and Special Interest and Resilience, respectively. In contrast, the Analyst community's interest lies in Security Architecture, followed by Security Operations, Threat Intelligence, and Special Interest and Resilience. On average, analysts tended to be much more interested in threat intelligence, likely due to the focused nature of their work.



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.