TLP: CLEAR

# Retail & Hospitality Industry Insights

## 2025 Verizon Data Breach Investigation Report Analysis

RETAIL & HOSPITALITY ISAC

# Introduction

With more than 300 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 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 2024 across industries included the emergence of fraud as one of the top threats facing members, and the continued prevalence of both vulnerability exploitation and AI-related threats.

# Executive Summary

As in previous years, 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 and ransomware remained top threats as reported by both Verizon and RH-ISAC Core Members
- While credential theft remained the top threat in Verizon data, for RH-ISAC fraud activity tied with phishing (note: many types of fraud activity leverage stolen credentials)
- Vulnerability exploitation also emerged as a top threat in Verizon data, but did not emerge as a key trend reported by RH-ISAC Core Members
- In Verizon data, top targeted industries aligned with RH-ISAC Core Members included manufacturing (2nd most targeted), wholesale (5th most targeted), and retail (7th most targeted), while the top reporting industries in RH-ISAC data are (in order of most targeting): retail, restaurants and food service, hospitality, and travel
- Cyber risks from the proliferation of AI tools remained a major concern in both Verizon and RH-ISAC datasets

For comparison, key points of comparison from the report covering 2023 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

# Verizon DBIR
# Key Takeaways

# Key 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 observed in 2024:

| | |
|---|---|
|  | Exploitation of **vulnerabilities as an initial access** step for a data breach grew by 34%, now accounting for 20% of breaches |
|  | **Ransomware** prevalence rose 37% from 2023, accounting for 44% of all breaches |
|  | 30% of all breaches involved a **third-party compromise**, nearly doubled from 2023 numbers |
|  | Roughly 28% of state-sponsored incidents had a **financial motive** |
|  | 60% of all breaches involved a **human element**, especially credentials stolen via social engineering, down roughly 8% from 2023 |

For comparison, the key findings for 2023 were:

- 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, roughly the same as 2022
- Third Party breaches represented 15% of all incidents
- Business email compromises (BEC) accounted for one fourth of financially motivated attacks

# Key Industries

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

| Industry | Incidents 2024 | Incidents 2023 | Confirmed Breaches 2024 | Confirmed Breaches 2023 |
|---|---|---|---|---|
| Accommodation & Food Service | ↓211 | 220 | ↓48 | 106 |
| Agriculture | ↑80 | 79 | ↓55 | 56 |
| Entertainment | ↑493 | 477 | ↑306 | 293 |
| Manufacturing | ↑3,837 | 2,305 | ↑1,607 | 849 |
| Retail | ↑837 | 725 | ↑419 | 369 |
| Transportation | ↑361 | 260 | ↑248 | 138 |
| Wholesale Trade | ↑330 | 76 | ↑319 | 54 |

# Geographic Regions

Verizon also provided key data for several geographic regions observed in 2024:

| | Frequency | Top Patterns | Threat Actors | Actor Motives | Data Compromised |
|---|---|---|---|---|---|
| **Asia-Pacific** | 2,687 Incidents<br>1,374 with confirmed data disclosure | 97% of breaches:<br>System Intrusion<br>Social Engineering<br>Basic Web Application Attacks | External - 99%<br>Internal - 1% (breaches) | Financial - 83%<br>Espionage - 34% (breaches) | Internal - 78%<br>Secrets - 33% |
| **Europe, Middle East, and Africa** | 9,062Incidents<br>5,321 with confirmed data disclosure | 89% of breaches:<br>Miscellaneous Errors<br>System Intrusion<br>Social Engineering | External - 71%<br>Internal - 29% (breaches) | Financial - 87%<br>Espionage - 18% (breaches) | Internal - 62%<br>Personal - 49%<br>Other - 37%<br>Secrets - 13% |

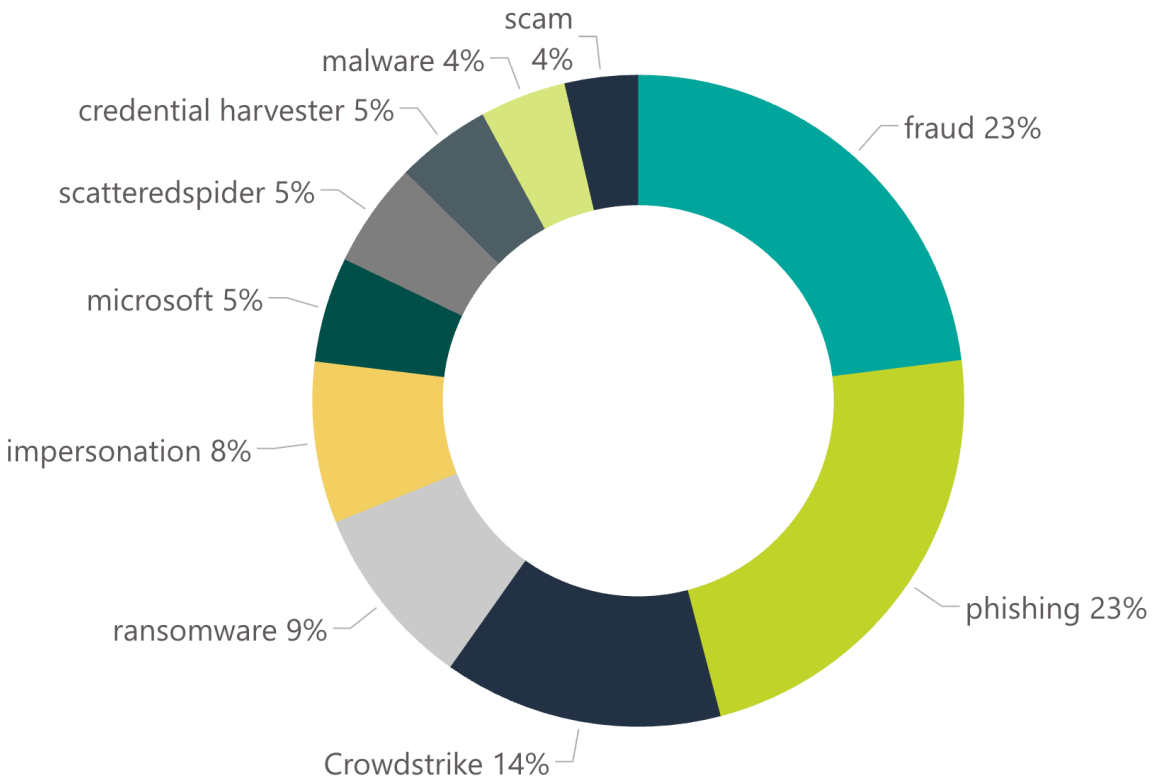
This data shows key increases for each region when compared to 2023 data:

- Incidents in the Asia-Pacific (APAC) region increased from 2,130 to 2,687, with confirmed breaches more than doubling from 523 to 1,374
- Incidents in the Europe, Middle East, and Africa (EMEA) region also increased exponentially from 8,302 to 9,062, with confirmed breaches dropping from 6,005 to 5,321

# RH-ISAC
# Sharing Trends

# Top Threat Trends

This graph illustrates the RH-ISAC community's shared threat trends for 2024, which can be described as the frequency that threats were shared through Member Exchange and Slack:




For comparison, in 2023, key trends included:

- Credential harvesting fell significantly, overtaken by other trends.
- Phishing retook first place at 25% of reported threats
- AI threats (15%), Fraud (15%), and Ransomware (14%) rounded out the remaining significant threat trends

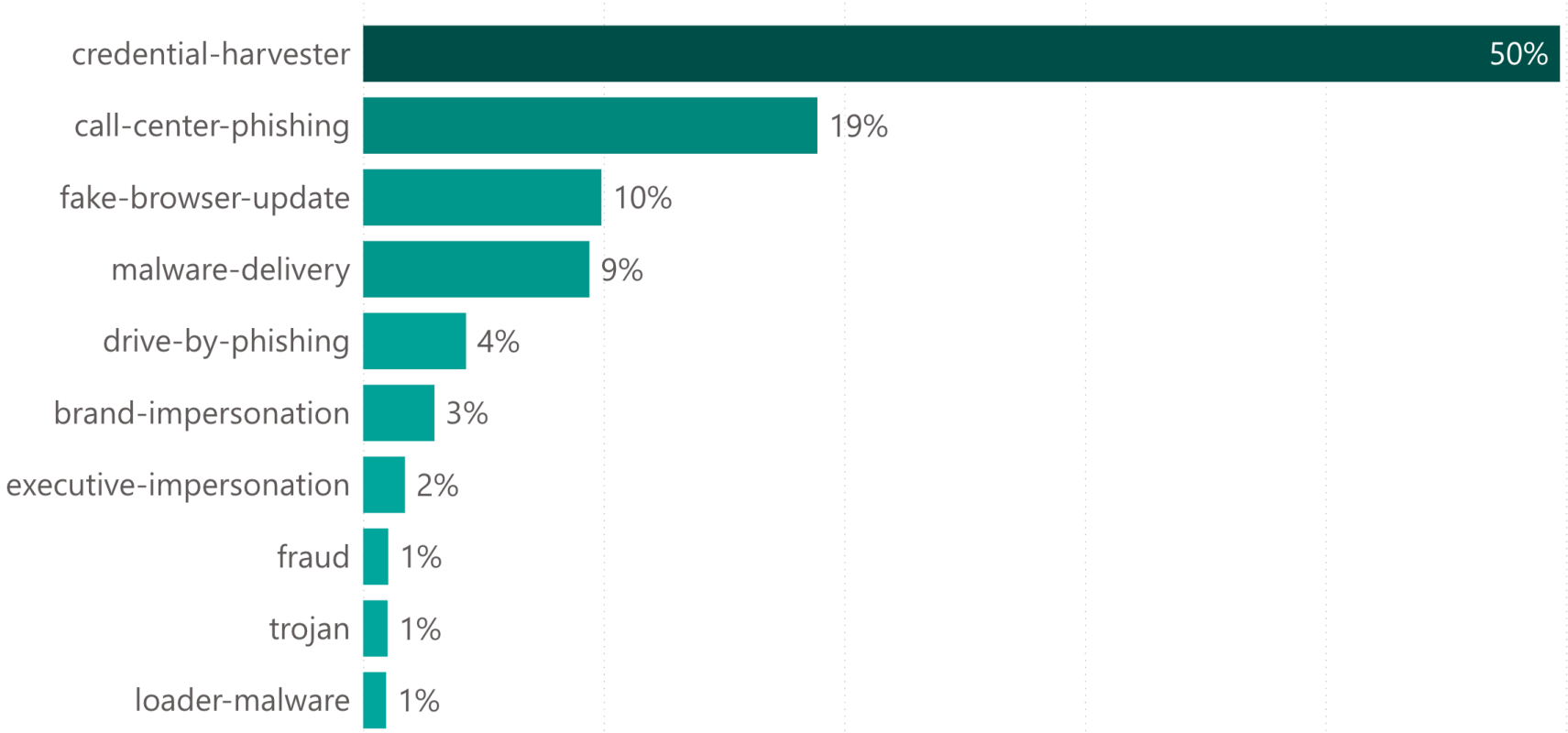
As with 2023, the Top Shared Trends for 2024 largely corroborate Verizon's primary findings that phishing and ransomware are among the most prominent initial infection threats facing organizations in the retail, hospitality, and travel sectors.  Fraud remained a critical concern, rising to tie with phishing as the most-reported threat.

# Top MISP Sharing Themes

For the period of January 1 – December 31, 2024, members published 4,712 events to MISP, including 51,094 unique attributes, compared to 2,568 events and 50,199 attributes in 2023. In addition to previously tracked data, the RH-ISAC Intelligence team is now able to track sharing in two new categories: threat types and industries.

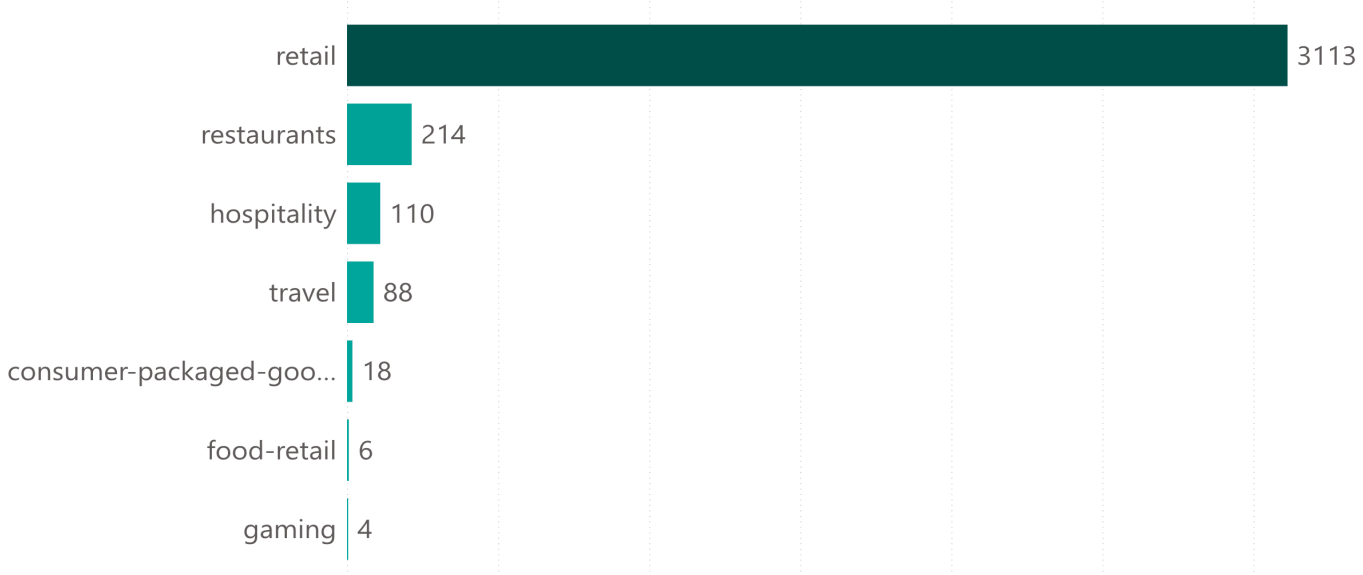
## Top Reported Threat Types

The top reported types of threats by members for the current period by total count of instances for 2024 were:



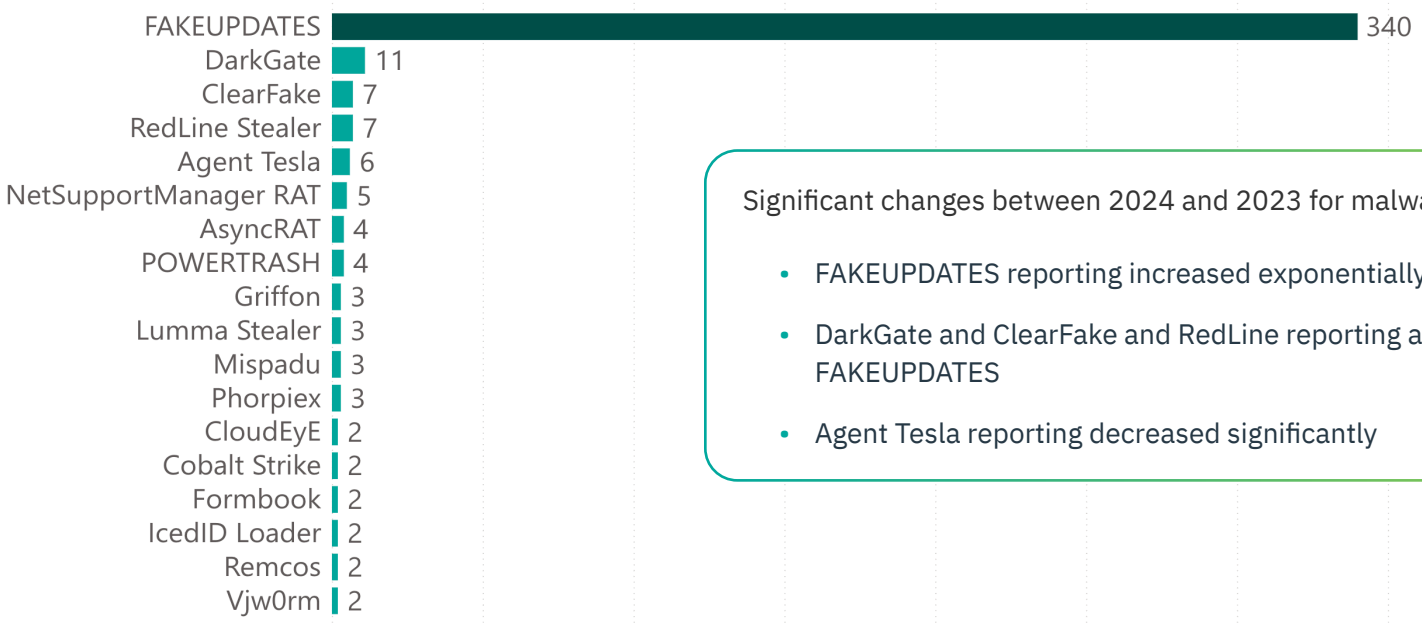
## Industry Breakdown

The share of intelligence reporting in MISP by members broken down by industry vertical by total count of instances for 2024 is as follows:




## Malware & Tools

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

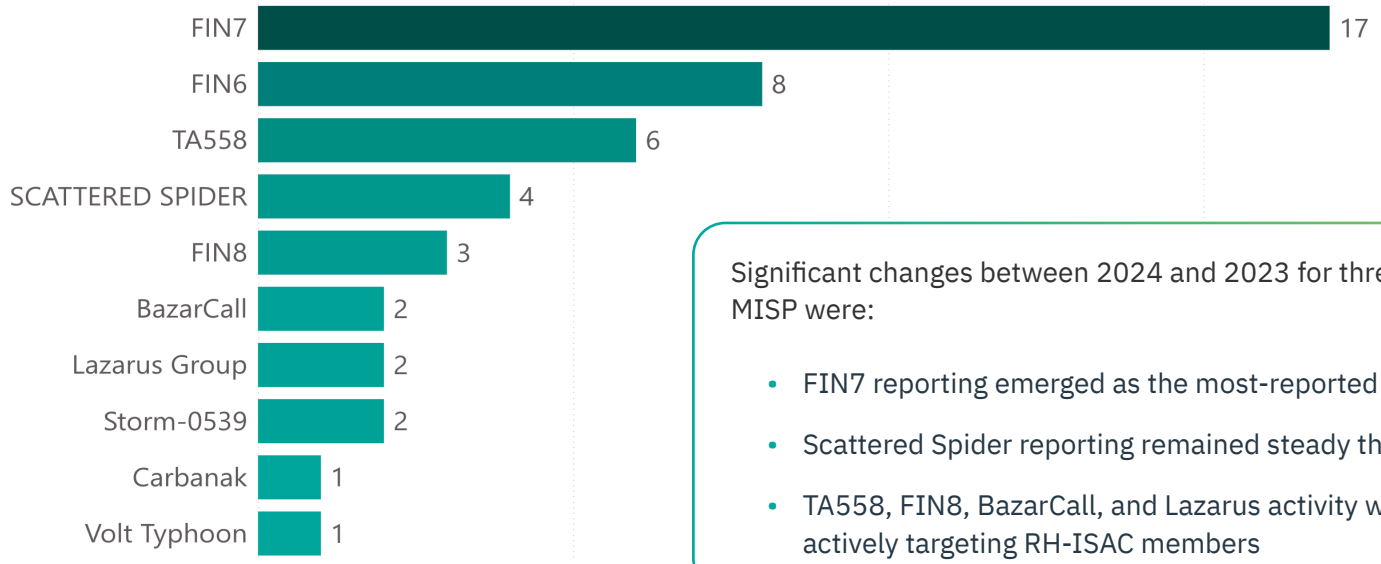



Significant changes between 2024 and 2023 for malware reporting in MISP were:

- FAKEUPDATES reporting increased exponentially, eclipsing all other malware
- DarkGate and ClearFake and RedLine reporting also increased at a lower rate than FAKEUPDATES
- Agent Tesla reporting decreased significantly

## Threat Actors & Instrusion Sets

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

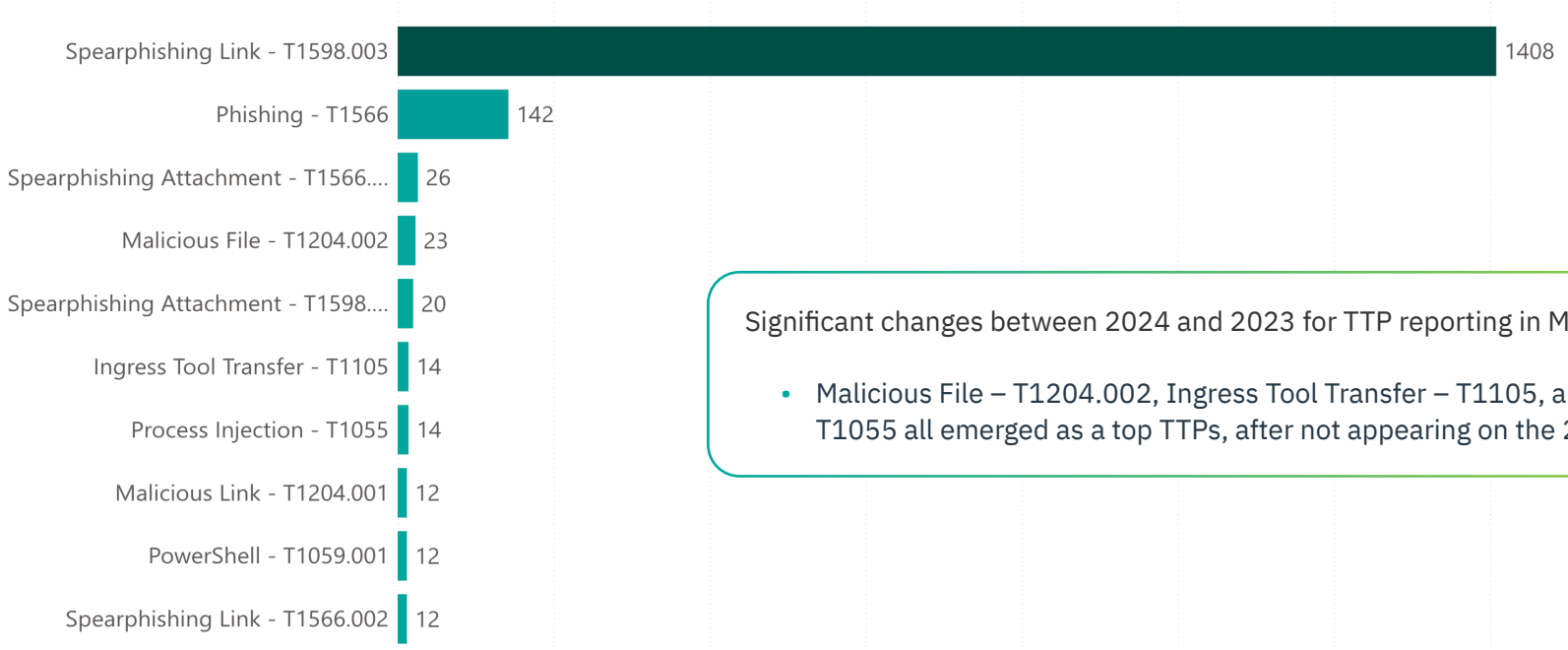



Significant changes between 2024 and 2023 for threat actor and intrusion set reporting in MISP were:

- FIN7 reporting emerged as the most-reported threat group, followed closely by FIN7
- Scattered Spider reporting remained steady throughout 2024
- TA558, FIN8, BazarCall, and Lazarus activity was less prevalent in 2024, but still actively targeting RH-ISAC members

## TTPs

The following graph demonstrates the most common MITRE ATT&CK Techniques reported by members:

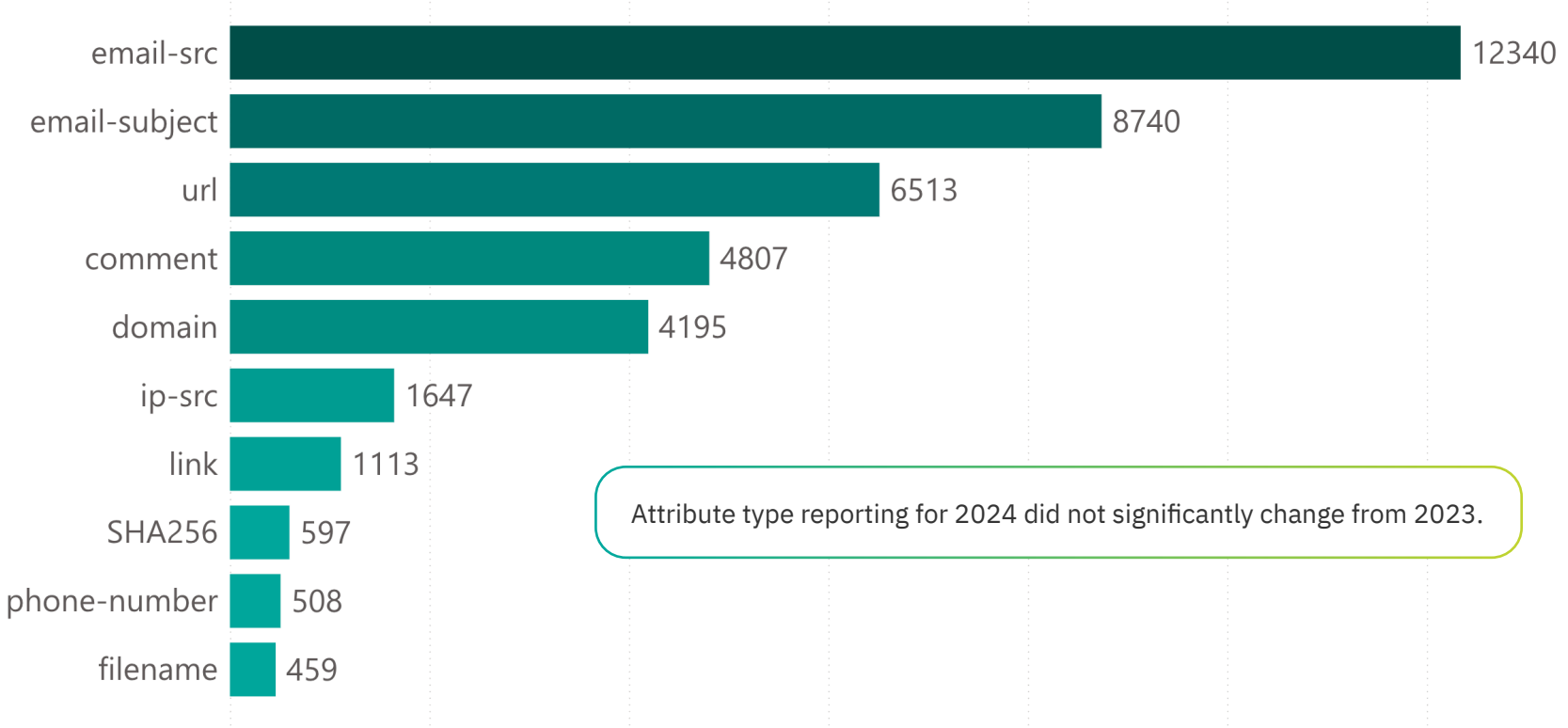



Significant changes between 2024 and 2023 for TTP reporting in MISP were:

- Malicious File – T1204.002, Ingress Tool Transfer – T1105, and Process Injection – T1055 all emerged as a top TTPs, after not appearing on the 2023 list

## Top Attributes

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




Attribute type reporting for 2024 did not significantly change from 2023.

# Associate Member
# **Industry Insights**

# Attack Trends for Retail and Hospitality

**For this year's release of the annual Verizon DBIR comparison report, RH-ISAC asked Associate Member Palo Alto Networks to contribute insights their intelligence team has for the retail, hospitality, and travel industries for 2024. Their analysis is included below.**

## Observations From the 2025 Unit 42 Global Incident Response Report

The 2025 Unit 42 Global Incident Response Report tracks insights from Palo Alto Networks consultants' observations of real life cases, combined with aggregated data from cases overall.

In this report, Unit 42 tracked the most common investigation types associated with key industries. For wholesale and retail, network intrusion topped the list. We use this classification when intrusion into the network is the only malicious activity we observe. The prevalence of this investigation type is in some ways good news, since it indicates that clients are calling us earlier in the attack chain, which can lead to stopping attackers before they have a chance to succeed at other objectives.

The report shows significant presence of business email compromise, extortion and ransomware, and a small but growing trend of cloud control plane compromise. Palo Alto Networks recently published observations of extortion and ransomware trends for the first quarter of 2025 on the Unit 42 Threat Research Center.

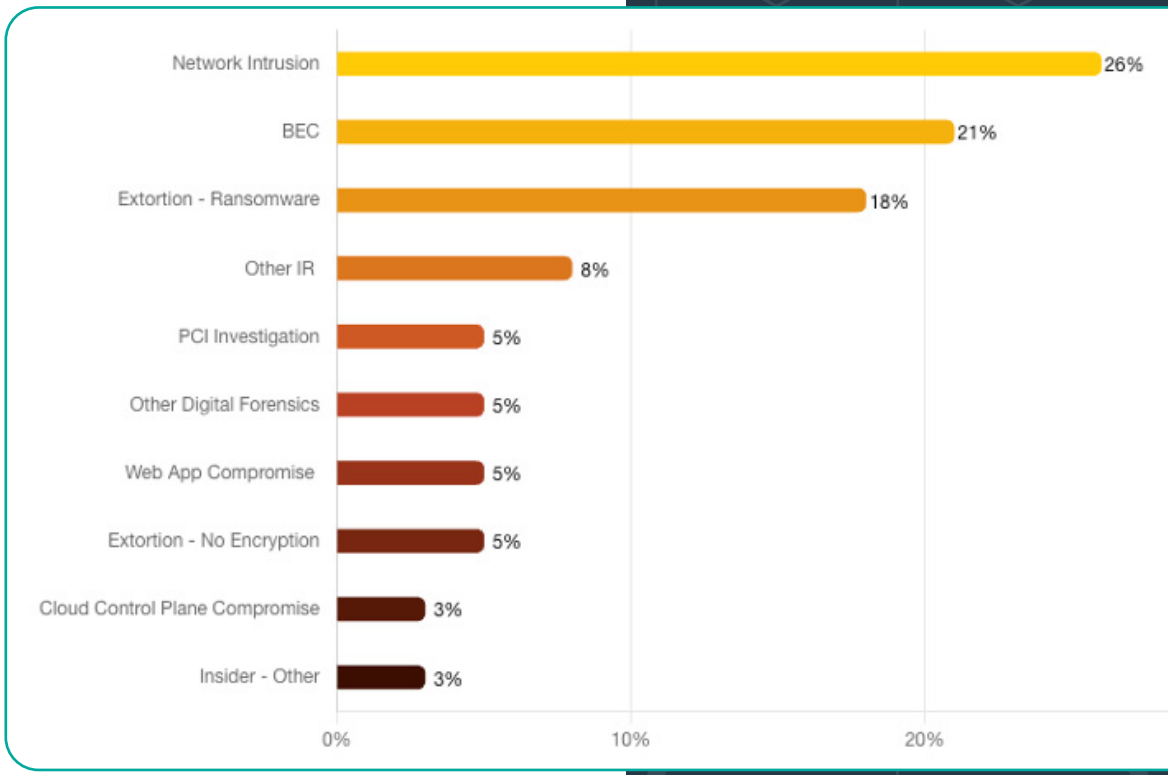



*Figure 1. Intrusion types observed for wholesale and retail organizations in the 2025 Unit 42 Global Incident Response Report.*

Unit 42 also tracks initial access vector for our incident response cases. In the most recent report, phishing was the most common initial access vector (23% of incidents). However, this was followed closely by software/API vulnerabilities (19% of incidents).

When the data is broken out by industry, phishing and software/API vulnerabilities are neck and neck for the wholesale and retail industries (25% each). However, it should be noted that some initial access vectors that are less prominent for other industries, such as the use of removable media, valid cloud accounts, and various types of misuse of credentials, including unsecured credentials and credentials from password stores.

Attacks are also growing in complexity. The most recent report looks into how threat actors pursued their objectives. It observed that they often pivoted from social engineering to attacking endpoints, cloud resources and others.

In 84% of incidents, threat actors attacked their intended victim across multiple fronts. 70% of the time, they did so across three or more. In some incidents we responded to, threat actors attacked across as many as eight fronts.

To combat this, Unit 42 incident responders had to access multiple types of data sources to complete their investigation. Defenders should prepare to efficiently process information from various sources to truly gain insight into possible attacks and mitigate them fully.

In addition to these insights, our 2025 Unit 42 Global Incident Response Report details emerging trends in the threat landscape. This includes statistics on the scale of business disruption in ransomware and extortion attacks, information on software supply chain and cloud attacks, charts showing the growing speed of intrusions and exfiltration, details on insider threats and early observations of AI-assisted attacks. For more information, please view the full 2025 Unit 42 Global Incident Response Report.

*Figure 2. Fronts of attack where we saw threat actors operating, from the 2025 Unit 42 Global Incident Response Report.*

| Fronts of Attack | % of Cases |
|---|---|
| Endpoints | 72% |
| Human | 65% |
| Identity | 63% |
| Network | 58% |
| Email | 28% |
| Cloud | 27% |
| Application | 21% |
| SecOps | 14% |
| Database | 1% |