

RH-ISAC COMMUNITY INSIGHTS FOR THE VERIZON 2026 DATA BREACH INVESTIGATION REPORT

Executive Summary

Each year, the RH-ISAC Intel Team compares intelligence sharing statistics and trends from the RH-ISAC Core Membership with findings in the Verizon Data Breach Investigation Report (DBIR). For 2025, most of RH-ISAC's findings corroborate Verizon reporting, with one key outlier: RH-ISAC membership continued to report social engineering and fraud tactics as the most prevalent threat vectors their companies face, while the Verizon report found that vulnerability exploitation outpaces social engineering. The Verizon report also emphasized the impacts of generative AI and Famous Chollima activity on the global cyber landscape, which were also common themes in RH-ISAC reporting.

Verizon 2025 Threat Landscape

For 2025, [key findings from the Verizon DBIR](#) included:

BREACHES AND THREATS

- 31% of breaches in 2025 resulted from software vulnerabilities
- 48% of all breaches in 2025 involved ransomware, but that payout rates by victims reduced drastically
- A significant increase in generative AI being leveraged by threat actors
- Click rates on mobile phishing in 2025 were 40% higher than computer click rates, and that threat actors largely pivoted to mobile device targeting for social engineering
- Famous Chollima activity ramped up significantly

VERIZON'S TARGETED

- Manufacturing (fourth most targeted with 3,627 attempted incidents)
- Wholesale (ninth most targeted industry with 1,057 attempted incidents)
- Retail (10th most targeted industry with 997 attempted incidents)
- Entertainment (15th most targeted industry with 587 attempted incidents)
- Accommodation (18th most targeted industry with 319 attempted incidents)

RETAIL BREAKDOWN

- System intrusion, basic web application attacks, and social engineering represented 95% of breaches
- 99% of breaches were initiated by external threat actors
- Affected data included 84% internal, 26% credentials, 20% secrets
- Initial access vectors included 42% vulnerability exploits, 14% credential abuse, 9% phishing

GLOBAL REGIONS

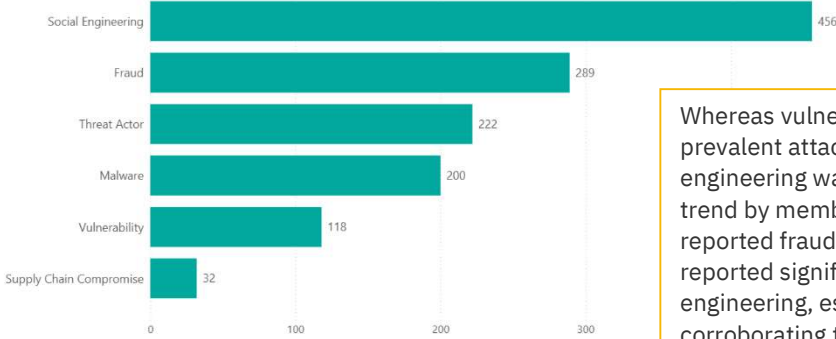
- The North American region experienced 12,371 attempted incidents and 8,246 confirmed breaches
- The EMEA region experienced 8,245 attempted incidents and 6,060 confirmed breaches
- The APAC region experienced 5,229 attempted incidents and 2,855 confirmed breaches
- The Latin American region experienced 813 attempted incidents and 718 confirmed breaches

RH-ISAC 2025 Threat Landscape

For comparison, below are the 2025 threat trend findings from RH-ISAC.

Top Sharing Trends

Sourced from RH-ISAC Core Member sharing.

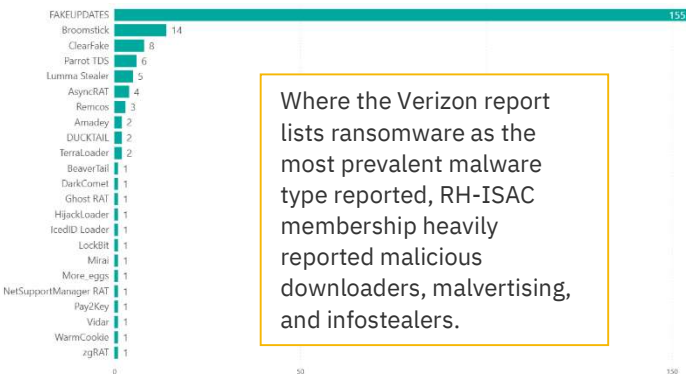


Whereas vulnerability exploitation was the most prevalent attack type reported by Verizon, social engineering was the most widely reported threat trend by membership, which also heavily reported fraud activity. RH-ISAC Core Members reported significant increases in mobile social engineering, especially smishing and vishing, corroborating the Verizon report.

Top MISP Trends

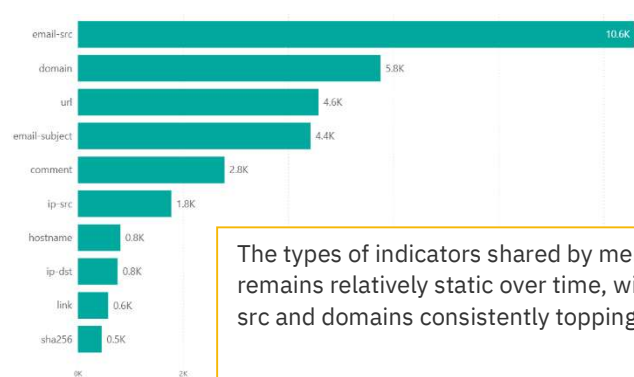
Sourced from RH-ISAC Core Member sharing.

MALWARE



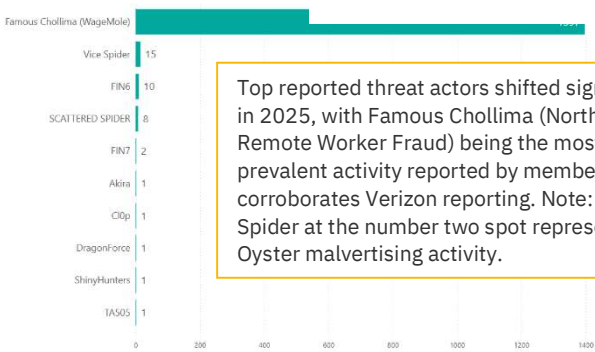
Where the Verizon report lists ransomware as the most prevalent malware type reported, RH-ISAC membership heavily reported malicious downloaders, malvertising, and infostealers.

ATTRIBUTE TYPES



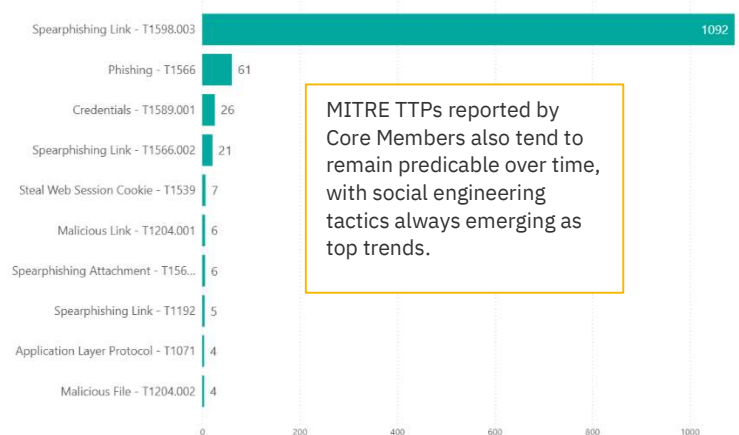
The types of indicators shared by membership remains relatively static over time, with email-src and domains consistently topping the list.

THREAT ACTORS



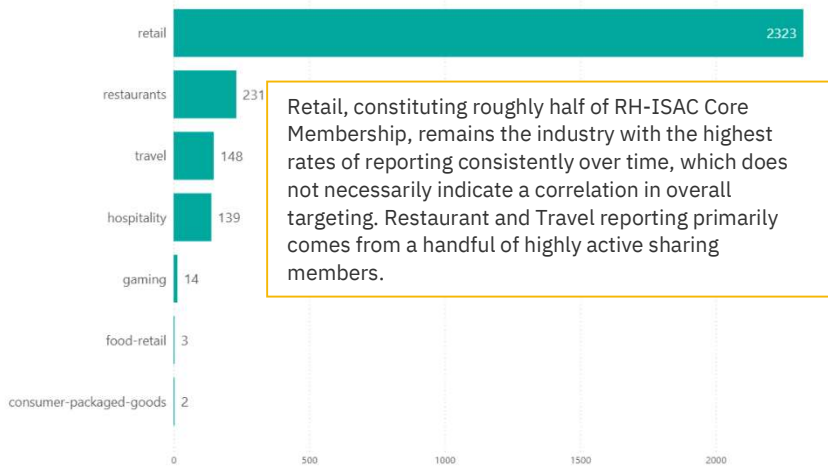
Top reported threat actors shifted significantly in 2025, with Famous Chollima (North Korean Remote Worker Fraud) being the most prevalent activity reported by members, which corroborates Verizon reporting. Note: Vice Spider at the number two spot represents Oyster malvertising activity.

MITRE ATT&CK TECHNIQUES



MITRE TTPs reported by Core Members also tend to remain predictable over time, with social engineering tactics always emerging as top trends.

MEMBER INDUSTRIES

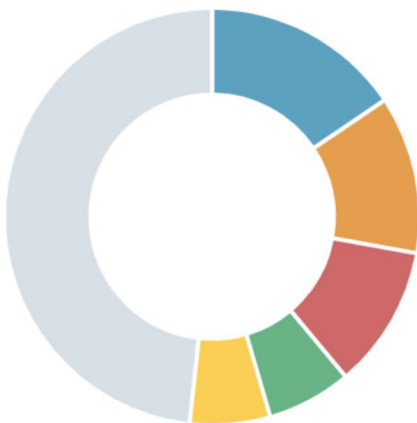


Retail, constituting roughly half of RH-ISAC Core Membership, remains the industry with the highest rates of reporting consistently over time, which does not necessarily indicate a correlation in overall targeting. Restaurant and Travel reporting primarily comes from a handful of highly active sharing members.

Top Industry Trends

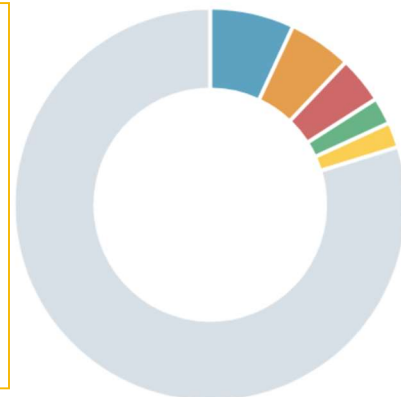
Sourced from Feedly Industry Tracking for industries within RH-ISAC purview.

Targeted industries



- Manufacturing Industry 16%
- Retail Industry 12%
- Media & Entertainment Industry 11%
- Telecom Industry 6%
- Travel & Hospitality Industry 6%
- Others 49%

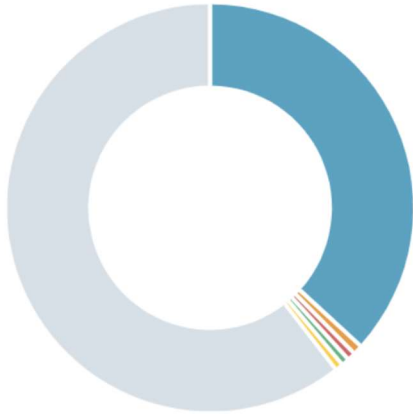
Most active malware



- AgendaCrypt 7%
- Akira 5%
- Clop 4%
- INC RANSOM 2%
- PLAY 2%
- Others 81%

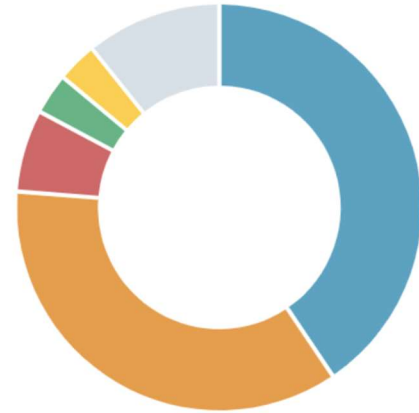
The “Other” industry category comprising nearly half of targeted industries is made up primarily of food and beverage, sports, and aviation reporting. The “Other” malware category is primarily infostealers, RATs, wiper, and DoS tools. Bohte charts largely confirm both Verizon and RH-ISAC findings.

Malware Types



● Ransomware 37% ● Keylogger 1% ● Bot 0%
● Backdoor Malware 0% ● Trojan Malware 0% ● Others 61%

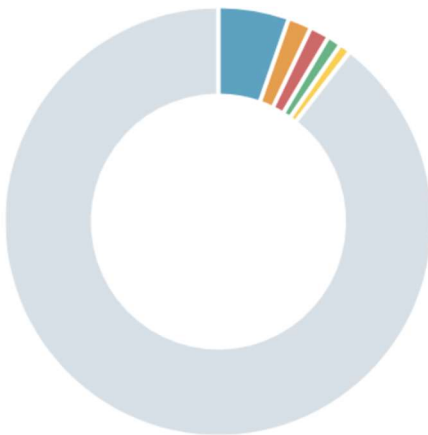
Attack Types



● Data Breaches & Exfiltration 41% ● Ransomware Attacks 36%
● Credential-Based Attacks 6% ● Social Engineering Attacks 3%
● DDoS & Service Disruption Attacks 3% ● Others 11%

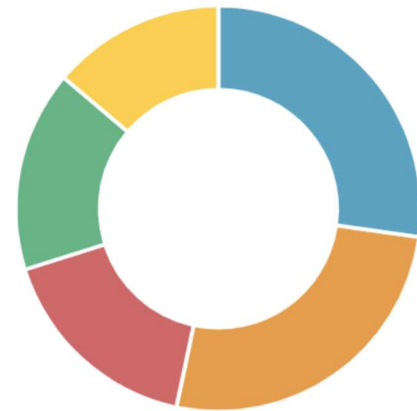
Attack type findings in Feedly reporting also skew heavily to data theft and ransomware, where RH-ISAC reporting more heavily reflects credential and social engineering attacks. RH-ISAC does not track reporting by company size, but generally, the more active sharing companies are larger and more resourced.

Most active threat actors



● Storm-1567 5% ● DragonForce 2% ● RansomHub 1%
● ShinyHunters 1% ● RansomHouse 1% ● Others 91%

Targeted companies by size



● Medium 27% ● Unknown 26% ● Large 17% ● Small 16%
● Enterprise 14%

The "Other" malware family category is divided among SafePay, DragonForce, Lync, and various ransomware strains. Note that the malware and threat actor findings emphasize ransomware far more than RH-ISAC membership reporting.