

RH-ISAC INTELLIGENCE TRENDS SUMMARY JANUARY-MARCH 2026

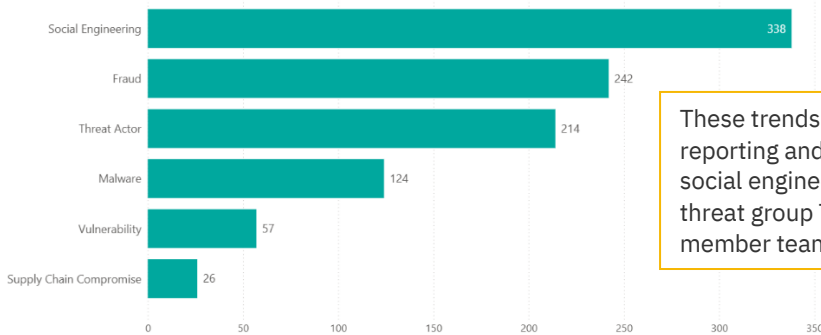
Executive Summary

Analysis of the intelligence sharing the first quarter of 2026 showed that the top reported threats by volume continued to reflect the steady reliance by threat actors on tried and tested threat vectors like fraud, social engineering, and malware. Member reporting heavily focused on Com-affiliated activity, widespread fraud activity, and cyber impacts of the Middle East conflict.

Threat Landscape

Top Sharing Trends

Sourced from RH-ISAC Core Member sharing.

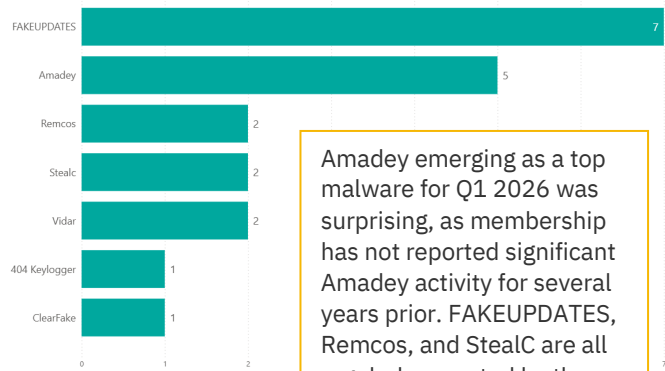


These trends tend to remain static over time in reporting and discussions on sharing platforms; social engineering, fraud activity, and specific threat group TTPs are always priorities for member teams.

Top MISP Trends

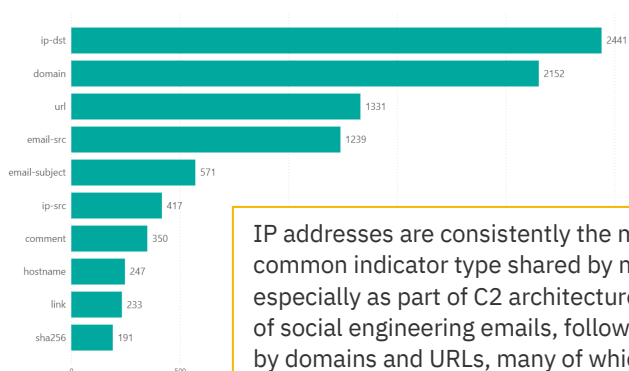
Sourced from RH-ISAC Core Member sharing

MALWARE



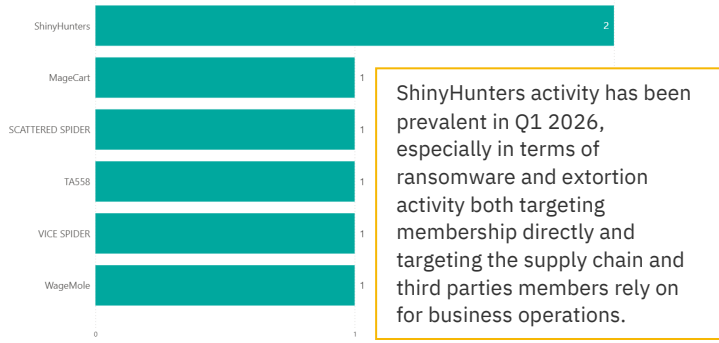
Amadey emerging as a top malware for Q1 2026 was surprising, as membership has not reported significant Amadey activity for several years prior. FAKEUPDATES, Remcos, and Stealc are all regularly reported by the membership.

ATTRIBUTE TYPES

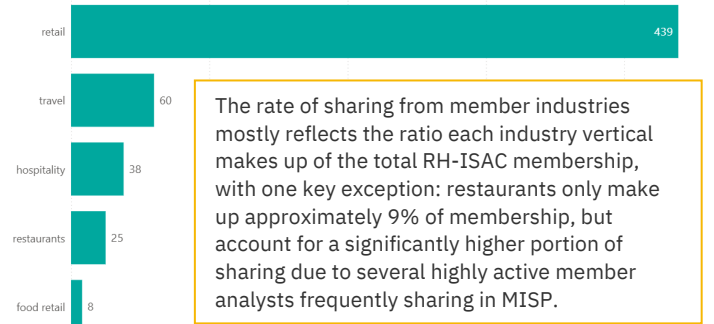


IP addresses are consistently the most common indicator type shared by members, especially as part of C2 architecture or senders of social engineering emails, followed closely by domains and URLs, many of which are often reported imposter domains looking to steal login credentials.

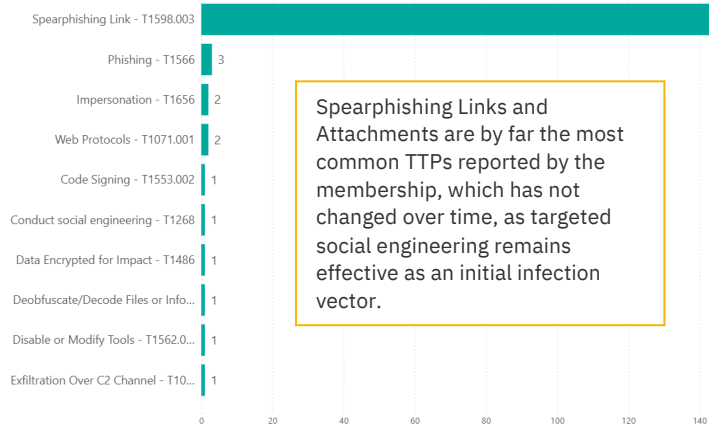
THREAT ACTORS



MEMBER INDUSTRIES



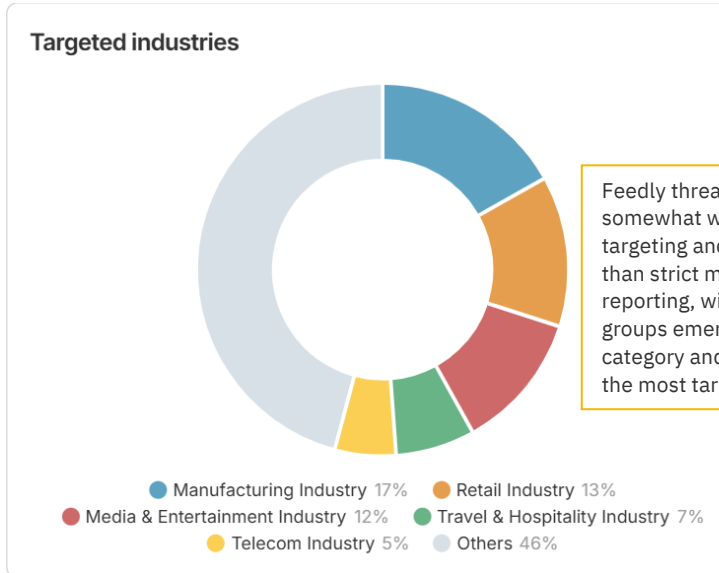
MITRE ATT&CK TECHNIQUES



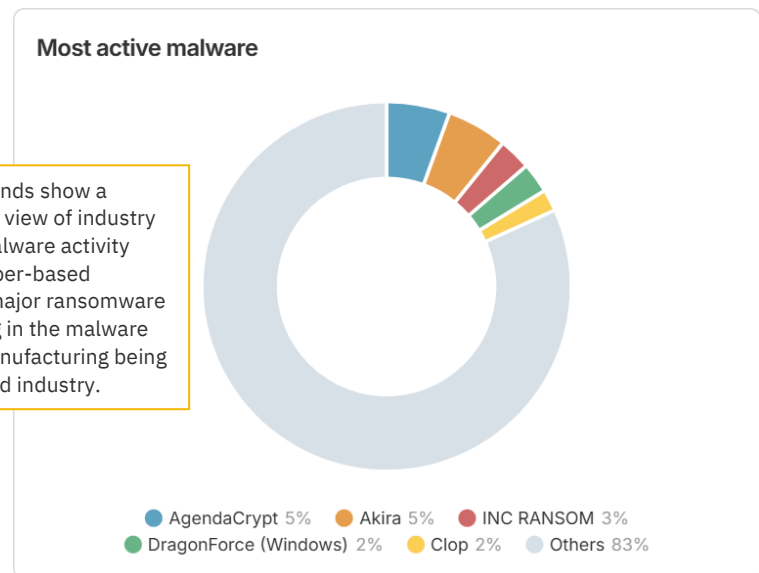
Top Industry Trends

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

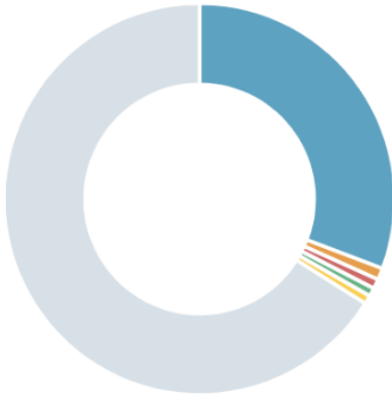
TARGETED INDUSTRIES



MOST ACTIVE MALWARE

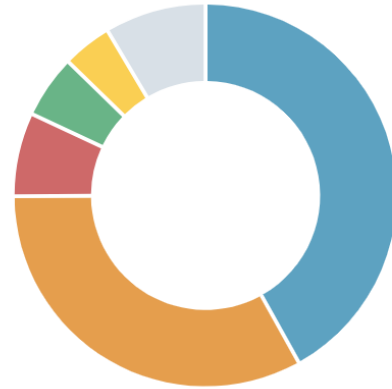


MALWARE TYPES



● Ransomware 31% ● Mobile Malware 1% ● Backdoor Malware 1%
● Trojan Malware 0% ● Wiper 0% ● Others 67%

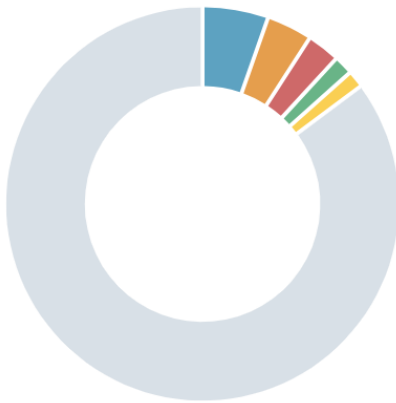
ATTACK TYPES



● Data Breaches & Exfiltration 42% ● Ransomware Attacks 33%
● Credential-Based Attacks 7% ● DDoS & Service Disruption Attacks 5%
● Web Application Attacks 4% ● Others 8%

Feedly also shows a more detailed view of the types of tools and attacks used by threat actors to target our industries, with ransomware and data breaches predictably leading the trends.

MOST ACTIVE THREAT ACTORS



● Storm-1567 5% ● The Gentlemen 4% ● DragonForce 3%
● ShinyHunters 1% ● RipperSec 1% ● Others 86%

TARGETED COMPANIES BY SIZE



● Medium 29% ● Unknown 24% ● Small 18% ● Large 17%
● Enterprise 13%

Feedly highlights several ransomware groups targeting our industries, all of which appear regularly in RH-ISAC dark web reporting. Feedly also shows a remarkably even spread of targeting by company size, indicating opportunistic rather than focused targeting.