TLP:CLEAR

RETAIL & HOSPITALITY ISAC

RH-ISAC INTELLIGENCE TRENDS SUMMARY APRIL-JUNE 2026

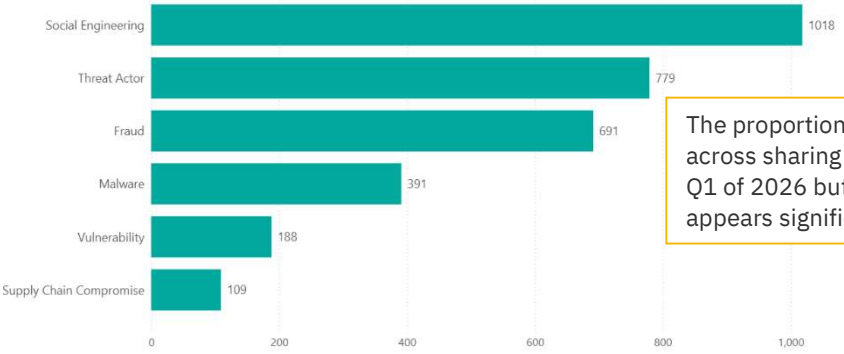
Executive Summary

Analysis of intelligence sharing during the second 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. Trends remain largely unchanged in Q2, outside of a surge in The Gentlemen ransomware activity and shifting malware prevalence.

Threat Landscape

Top Sharing Trends

Sourced from RH-ISAC Core Member sharing.

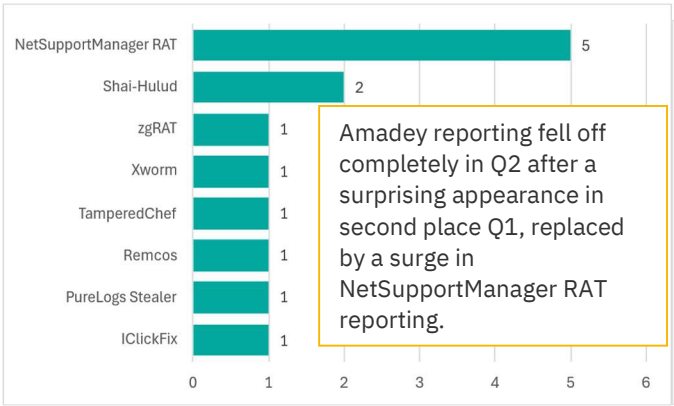


The proportion of discussion topic prevalence across sharing platforms has not changed since Q1 of 2026 but the total volume of shares appears significantly higher.

Top MISP Trends

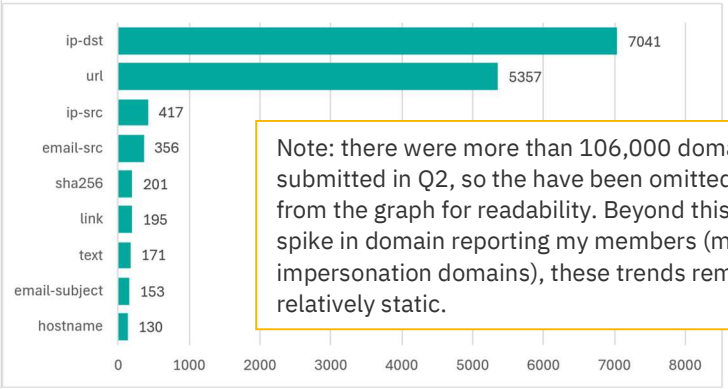
Sourced from RH-ISAC Core Member sharing

MALWARE



Amadey reporting fell off completely in Q2 after a surprising appearance in second place Q1, replaced by a surge in NetSupportManager RAT reporting.

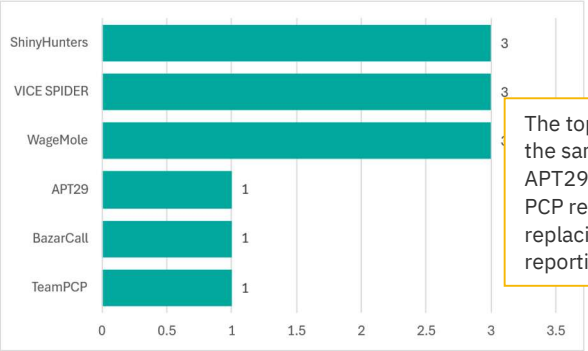
ATTRIBUTE TYPES



Note: there were more than 106,000 domains submitted in Q2, so the have been omitted from the graph for readability. Beyond this spike in domain reporting my members (mostly impersonation domains), these trends remain relatively static.

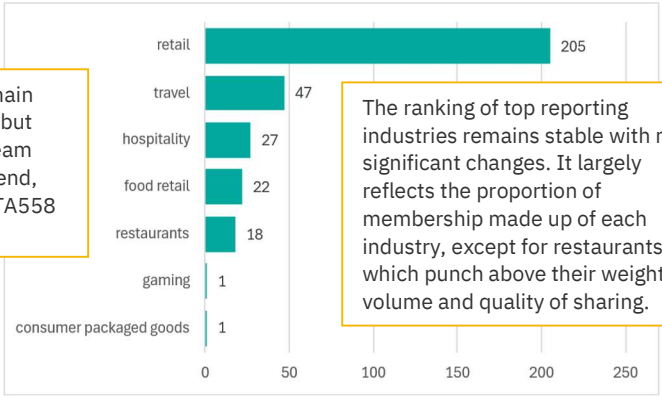
RETAIL & HOSPITALITY ISAC

THREAT ACTORS



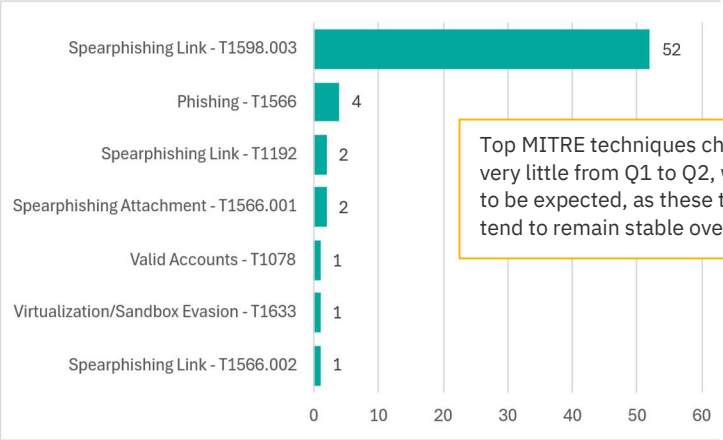
The top threat actors remain the same from Q1 to Q2, but APT29, BazarCall, and Team PCP reporting is a new trend, replacing MageCart and TA558 reporting in Q1

MEMBER INDUSTRIES



The ranking of top reporting industries remains stable with no significant changes. It largely reflects the proportion of membership made up of each industry, except for restaurants, which punch above their weight in volume and quality of sharing.

MITRE ATT&CK TECHNIQUES

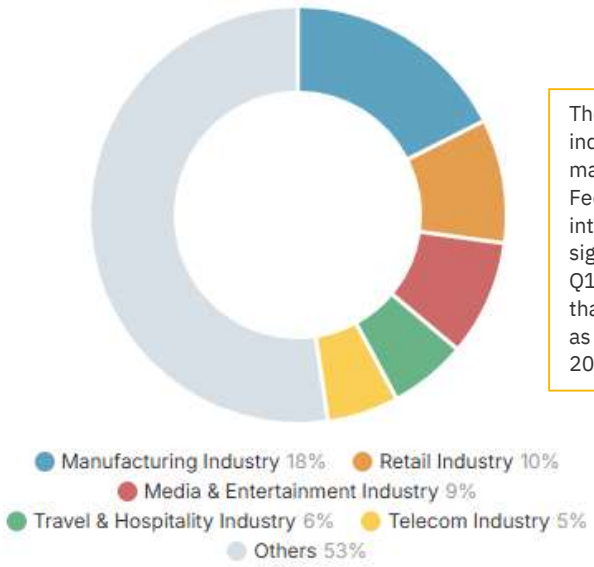


Top MITRE techniques changed very little from Q1 to Q2, which is to be expected, as these trends tend to remain stable over time.

Top Industry Trends

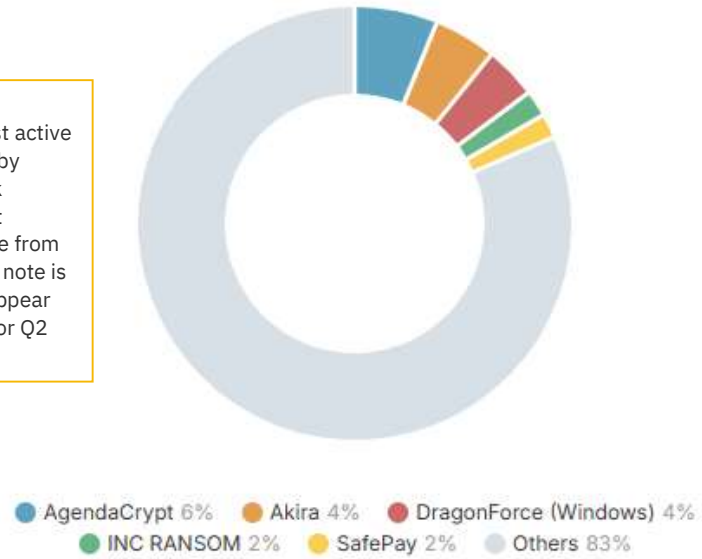
Sourced from Feedly Industry Tracking for industries within RH-ISAC purview.

TARGETED INDUSTRIES

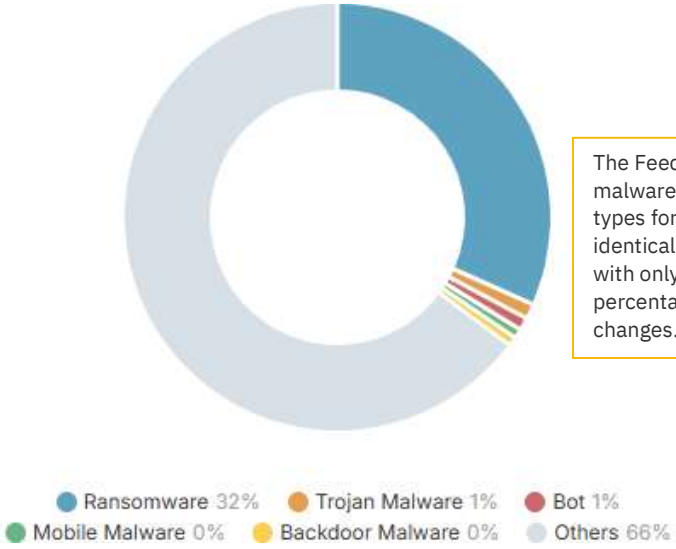


The top targeted industries and most active malware reported by Feedly cyberattack intelligence did not significantly change from Q1 to Q2. The only note is that Clop did not appear as a top malware for Q2 2026.

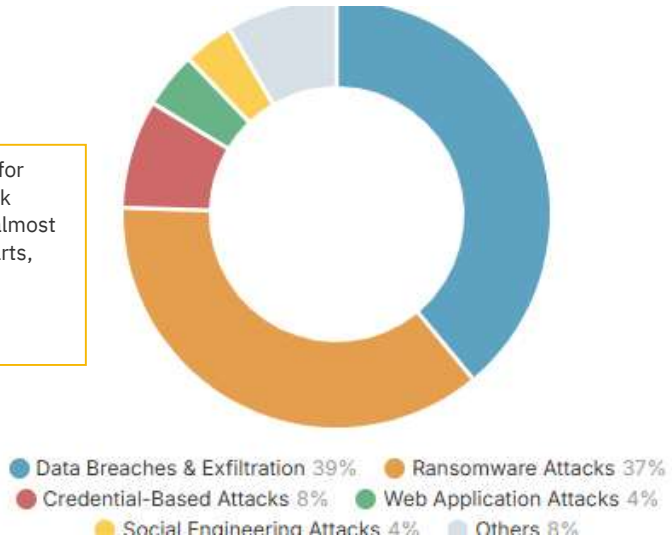
MOST ACTIVE MALWARE



MALWARE TYPES

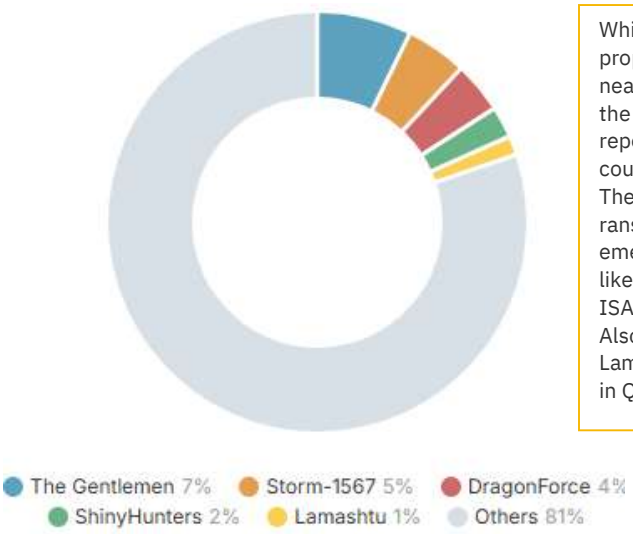


ATTACK TYPES

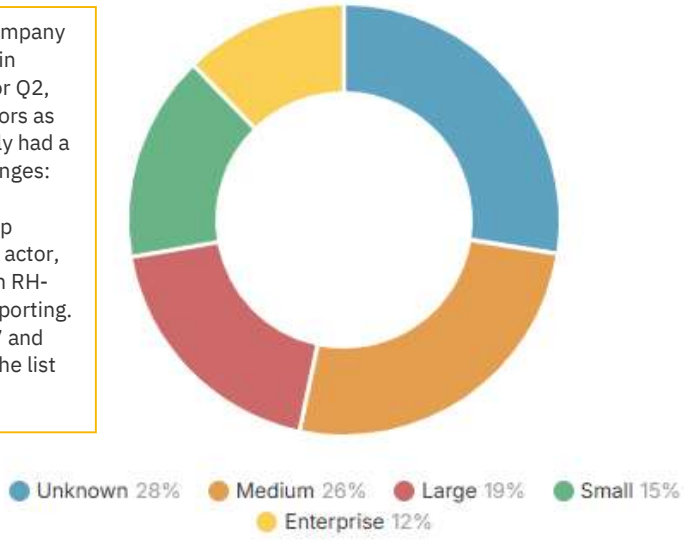


The Feedly charts for malware and attack types for Q2 look almost identical to Q1 charts, with only minor percentage point changes.

MOST ACTIVE THREAT ACTORS



TARGETED COMPANIES BY SIZE



While targeted company proportions remain nearly identical for Q2, the top threat actors as reported by Feedly had a couple of key changes: The Gentlemen ransomware group emerged as a key actor, like spikes seen in RH-ISAC dark web reporting. Also, Storm-1567 and Lamashtu made the list in Q2.