TLP: CLEAR

RETAIL & HOSPITALITY
ISAC

INTELLIGENCE TRENDS SUMMARY

January - April 2023

Introduction

In this installment of the RH-ISAC Intelligence Trends Summary, we highlight where intelligence sharing, requests for information (RFIs), surveys, and a wide variety of other engagements continued to provide insights into the major security concerns and challenges facing the community. This report looks back at the RH-ISAC community's intelligence-sharing output for the four-month period between January 1 and April 30, 2023. We shed light on the top threats and malware families reported by the community and try to extract trends and insights to help member analysts understand and detect shifts in the retail, hospitality, and travel threat landscape.

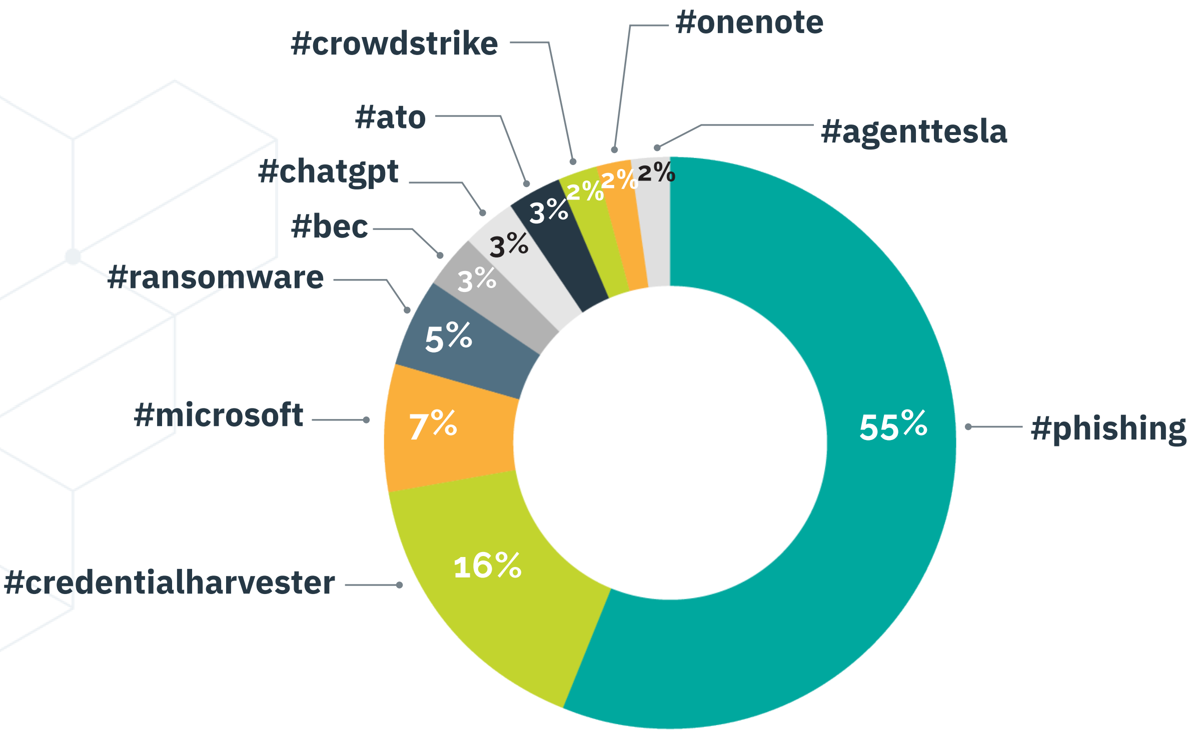
The RH-ISAC Research and Analytics team has also stayed busy supporting the community through the management and distillation of various requests for information (RFIs), surveys, and curating Communities in Member Exchange. From risk management to loyalty programs to security architecture, members in both communities engaged in enriching exchanges and produced practical and actionable content.

Analysis of the intelligence sharing for this period showed that the top reported threats by volume continued to reflect the steady reliance by cybercriminals on tried and tested threat vectors like credential harvesting and phishing. Agent Tesla remained a key threat, Emotet has reemerged after falling off during previous reporting periods, and familiar threats like IcedID and QakBot remain steady threats to the community. Key tactics leveraged against the community included Spearphishing links and attachments, and imposter and malicious domains. As familiar threats continue to shape the threat landscape for the retail, hospitality, and travel sectors, emerging trends shift the nuances and demands on resources for cyber defenders.

Top Sharing Trends

This graph illustrates the shared threat trends for the current period, which can be described as the frequency that threat types were shared through Member Exchange, Slack, and MISP. In the current period, phishing emerged as the most common threat at 55%, up from 31% as the second-most prominent threat from the prior reporting period. And credential harvesting fell significantly from 53% to 16%. For the September to December period, credential harvesting was the most common threat shared by members at 53%, which was up significantly from the previous period's 43%.

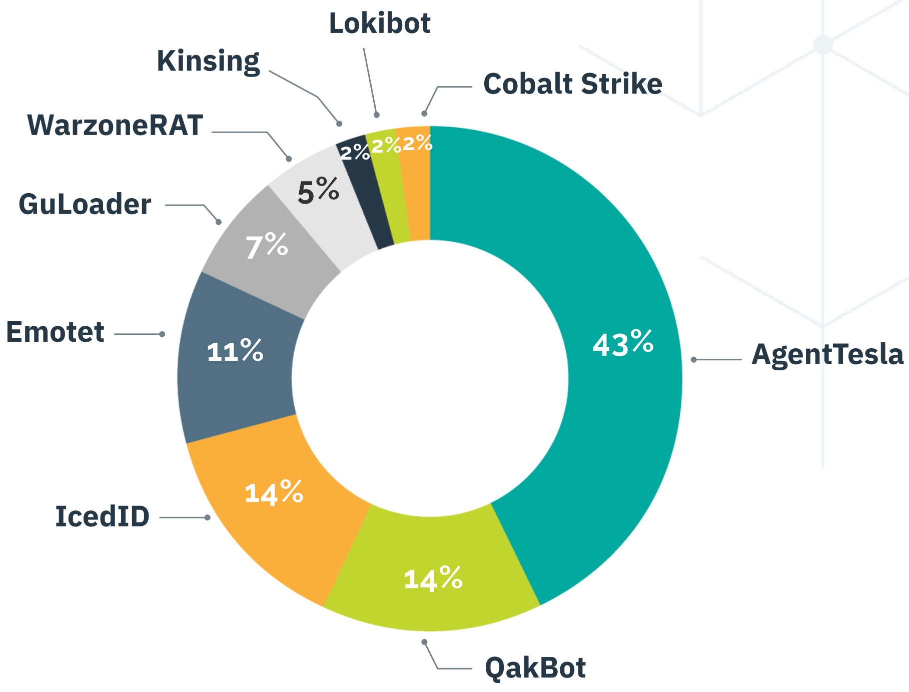
In third and fourth place are Microsoft (7%) and ransomware (5%), compared to SocGholish (5%), and Agent Tesla (4%) in the prior period. For January-April 2023, Agent Tesla came in 11th place at 2%, and SocGholish did not make the top list. In fifth place for the current period is Business Email Compromise (BEC) at 3%. Notable new trends for the period include OneNote (2%) and ChatGPT (3%).



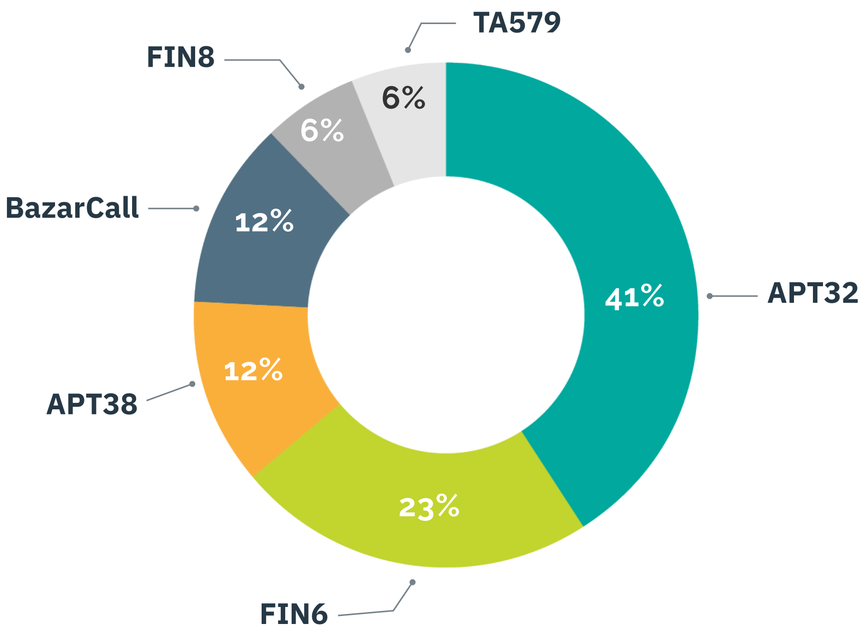
Top MISP Trends

Tracked data on member-reported threat trends includes prevalent malware, threat actors, intrusion sets, MITRE ATT&CK Techniques, and attribute types.

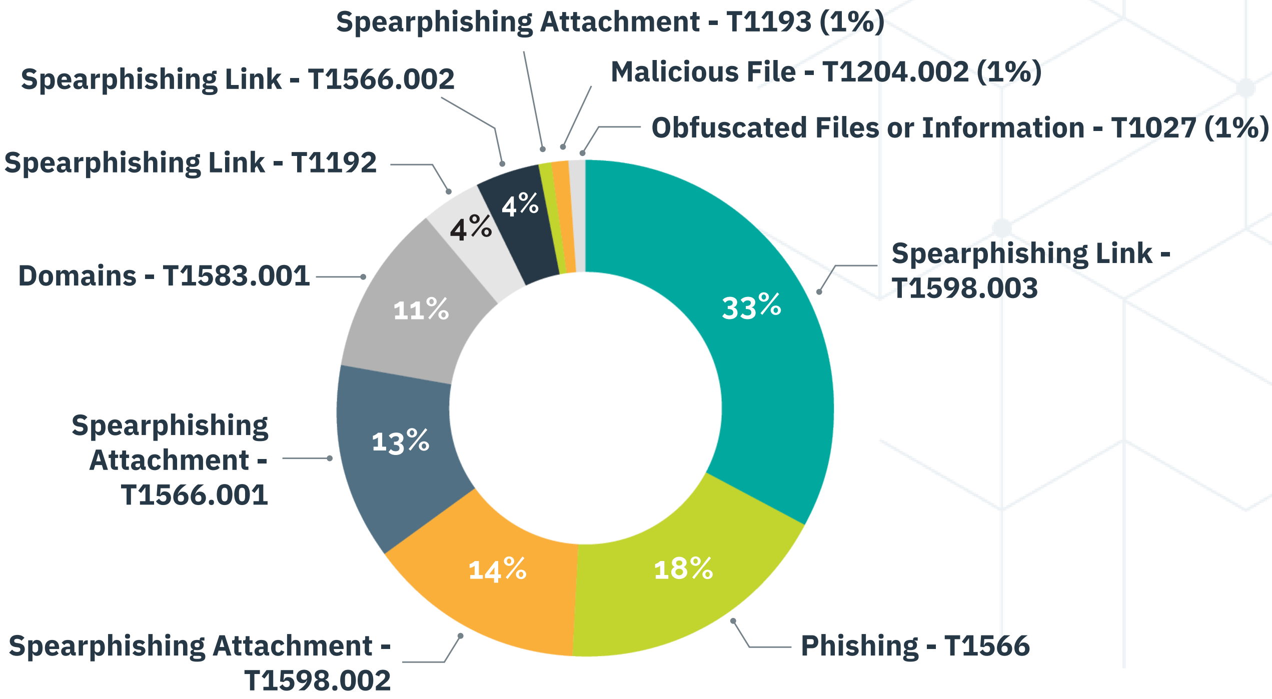
Top Reported Malware



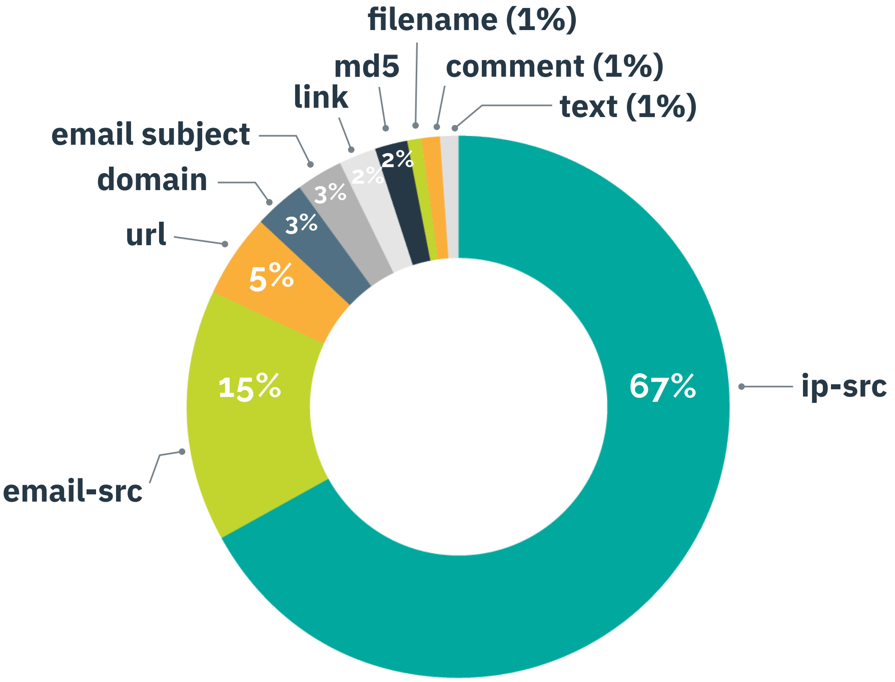
Top Reported Threat Actors & Intrusion Sets



Top 10 MITRE ATT&CK Techniques



Top 10 Attribute Types



Requests for Information

Members continue to leverage the RH-ISAC Request for Information (RFI) process integrated into Member Exchange, enabling our members to post RFIs to their peers with attribution or anonymously.

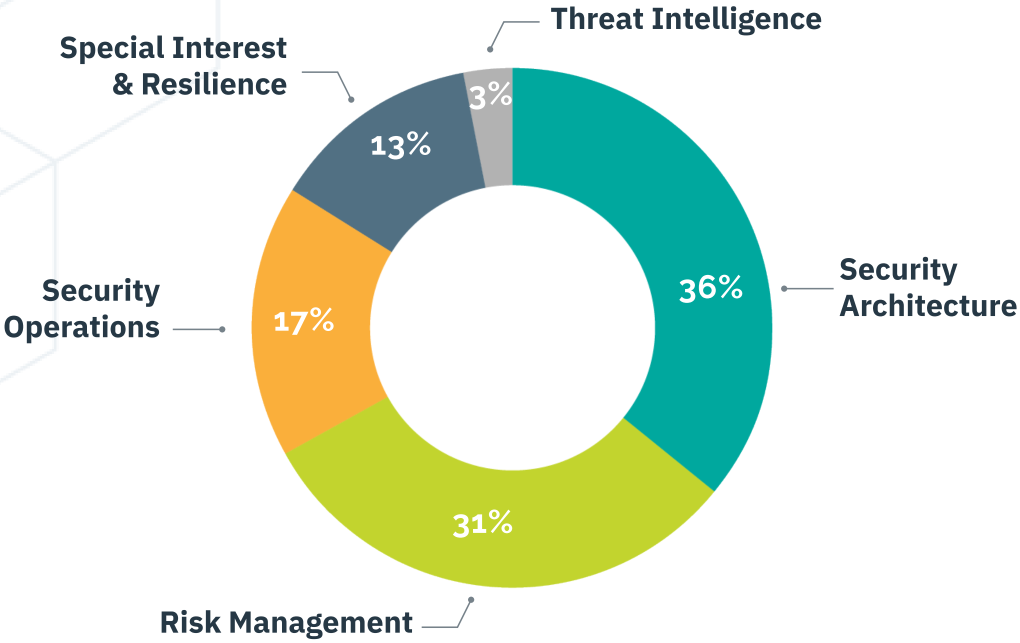
RH-ISAC has continued to track RFIs and surveys to determine what our members are most interested in, from the analyst perspective to the CISOs. Between January and April 2023, 133 unique members, or 49% of our total membership, participated in RFIs or surveys, indicating an interest in crowdsourcing information from peers within the same sector.

In total, for the timeframe of January to April 2023, 117 RFIs were submitted, with 274 responses. In addition, four domain-related surveys were conducted that generated 64 responses, including a Benchmark Study, the 2023 Tools and Technology Report that gathered 138 responses. The full report will be shared in late May or early June 2023.

Overall, from January to April 2023, 122 RFIs and surveys were submitted, with 476 responses.

Total RFIs/Surveys for January - April 2023

122 RFIs & Surveys | 476 Responses | Average Response: 4



Community Engagement Outlook

In 2022, for the timeframe of January to April, RH-ISAC received 64 RFIs that generated 161 responses. During 2023, continuous persistence, enhanced offerings, and growth in networking reflected an increase in community engagement with a spike in the numbers of RFIs (82%) and responses (70%).

CISO Community Overview

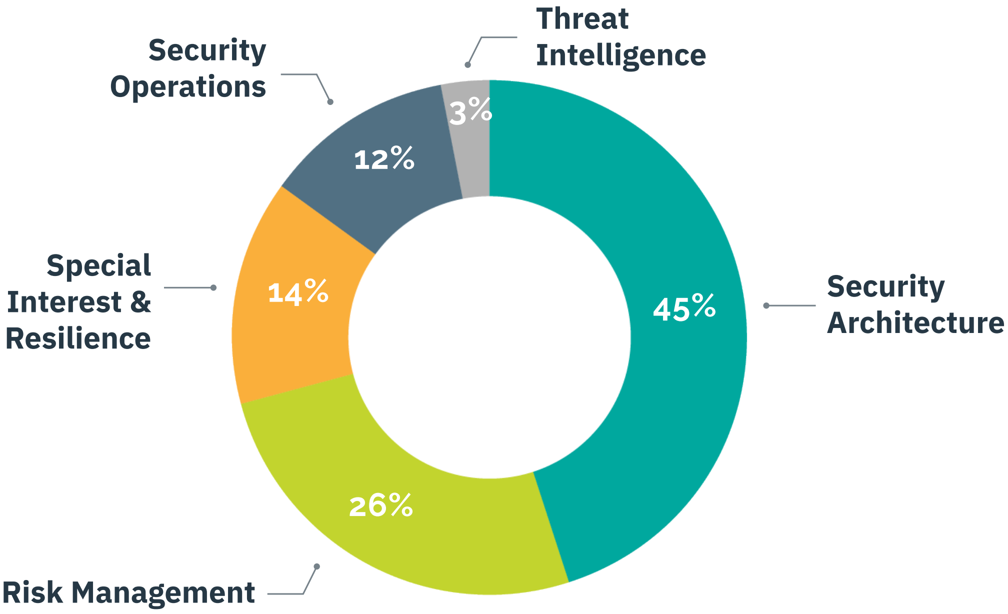
In the CISO Community, for January to April 2023, 58 RFIs were submitted, with 191 responses. During this period, 45% of the RFIs came from the security architecture domain, with greater interest in sub-domains such as identity & access management and security engineering (tool integrations & use cases).

Identity & access management discussed CIAM, PAM, and Loyalty topics. At the same time, security engineering involves questions about tools such as TrustARC, Red Canary, Twilio, Simeio, and job scheduling and automation solutions.

Another popular domain that contributed more than a quarter of RFIs was risk management (26%). Risk-related RFIs belong to frameworks and standards such as budgets and fraud function roles and responsibilities.

The figure below shows a total breakdown of the RFIs submitted to the CISO Community.

58 RFIs & Surveys | 191 Responses | Average Response: 3



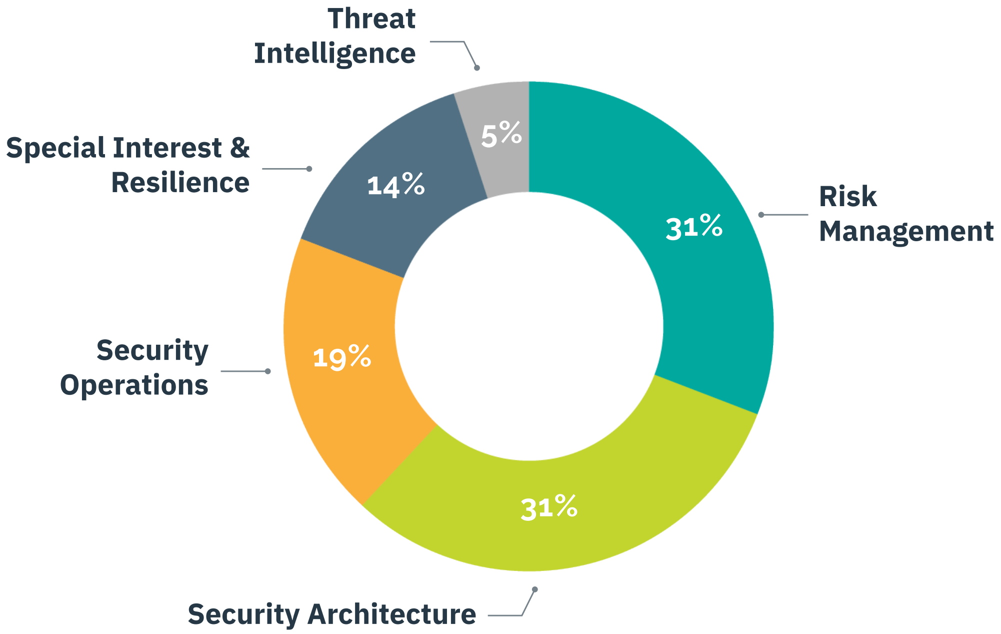
Analyst Community Overview

In the Analyst Community, for January to April 2023, 42 RFIs were submitted, with 66 responses. During this period, security architecture and risk management remained key discussion topics among the analyst community, together contributing 62% of overall RFIs.

Like the CISO community, RFIs from security architecture mainly belong to sub-domains identity & access management; discussing customer logins; account resets; loyalty points; and security engineering (tool integrations & use cases), covering tools such as Arkose, Mimecast, CyberGraph, OpenRefine software, and more.

The figure below shows a total breakdown of the RFIs submitted to the Analyst Community.

42 RFIs & Surveys | 66 Responses | Average Response: 1.5



Surveys

During January-April 2023, RH-ISAC conducted four surveys and one Benchmark Study.

BYOD Stipend Model for Personal Mobile Users

The Research & Education team distributed survey to the CISO and IAM community which aims to understand if fellow members are offering a stipend for the business use of a personal phone for corporate and non-corporate employees subjected to recent legislative policy in which the employer shall reimburse “all reasonably necessary expenses that are directly related to services performed for the employer.”

Business Continuity & Disaster Recovery (BC/DR)

The survey better understands BC/DR programs and determines if peers are shifting toward and/or defining business resiliency practices.

Configuration Management Database (CMDB)

The survey seeks to understand how RH-ISAC members have implemented a CMDB and what things should be considered when doing so.

Fleet Security Survey

The Research & Education team conducted a specialized survey within its unique group of fuel retailers in its membership. The survey aims to understand if fellow members allow usage of fleet cards at their retail fuel locations and how they are being protected.

According to the responses, a majority of retailers (80%) accept fleet cards; however, a small percentage (20%) allow mobile transactions.

Tools and Technology Benchmark Report

The RH-ISAC completed its third 2023 Tools and Technology Benchmark Report in April. It was fielded during the months of March and April 2023 and generated 101 unique responses, reflecting 42% participation from the overall membership.

The survey benchmarks security tools and technology that RH-ISAC members utilize. This includes endpoint/EDR, SIEM, TIP, SOAR, WEB PROXY/ WEB GATEWAY, Cloud Providers, Firewall or Network Security Appliances, MSSP/MDR vendors, and much more.

The RH-ISAC Sectors Threat Landscape

Key issues in the cyber threat landscape facing the retail, hospitality, and travel sectors remain complex and rapidly shifting. While new CVEs and threat actors emerge, old threat groups and tried-and true TTPs continue to strengthen or renew their prevalence.

Reporting Trends

During the current period, a series of high-profile topics and events dominated the cyber threat landscape globally and for the retail, hospitality, and travel sectors specifically. Key reporting for January-April 2023 included:

- Charming Kitten APT Targeting Multiple Global Regions with BellaCiao Custom Dropper Malware Campaign
- UPDATE: Mandiant Initial Analysis of 3CXDesktopApp Supply Chain Attack Confirms North Korean Threat Actor
- New Report Outlines Challenges in CTI for CISOs and Cyber Leaders
- FBI IC3 2022 Internet Crime Report Identifies Key BEC and Ransomware Trends
- Winter Vivern Cyberespionage Campaign Targeting Global Telecommunication and Government Organizations
- Social Engineering Scams Targeting Fashion and Brand Influencers Increasing in Prevalence and Sophistication
- Prilex POS Malware Targeting Contactless Credit Card Transactions
- RH-ISAC Adopts TLP 2.0 Standards

Leading reporting trends from the previous period included:

- Major cyber threats to operational technology and industrial control devices
- Major cyber threats facing the APAC community
- Major global events of relevance to member operations, such as the 2022 World Cup
- Major strategic trend reports affecting multiple industries
- Common malware and threats targeting members
- Major predictions and preparations from members regarding the 2022 Holiday season
- Skimming activity and other threats facing oil and gas retailers

RH-ISAC Threat Actor Profile Catalog

The Project

In February 2023, the RH-ISAC intelligence team published a catalogue of the most prominent and prolific threat groups targeting our community as a resource for member analysts. The catalogue is available via the RH-ISAC MISP instance and contains useful data on threat groups, including:

- Known aliases
- Background information and a brief history
- Prominent open source incidents attributed to the group
- Known tactics, techniques, and procedures (TTPs) leveraged by the group
- Any available indicators of compromise (IOCs) attributed to the group
- Data Sources