TLP: CLEAR

RETAIL & HOSPITALITY ISAC

INTELLIGENCE TRENDS SUMMARY

May - September 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 May 1 and August 31, 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 the Analyst and CISO communities engaged in enriching exchanges and produced practical and actionable content.

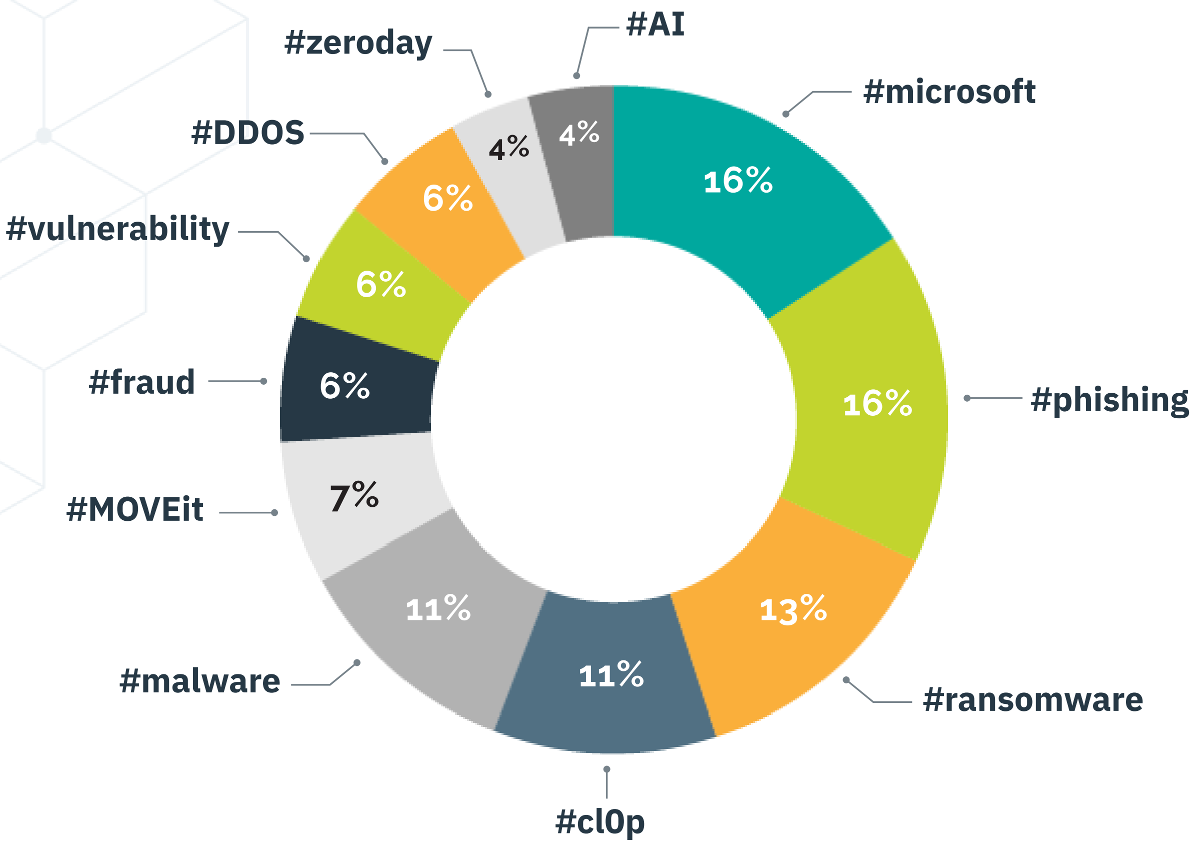
Analysis of the intelligence sharing for this period showed that the top reported threats by volume continued to reflect the steady reliance by cybercriminals on tried and tested threat vectors like phishing. Microsoft-related threats, ransomware strains, and various vulnerabilities emerged as key threats shared by members over the summer. 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 the RH-ISAC Malware Information Sharing Platform (MISP). In the current period, phishing emerged as the most common threat at 16%, down from 55% as the most prominent threat from the prior reporting period (Jan-April 2023). Interestingly, generalized credential harvesting fell off the list entirely from 16% the prior period. For the January to April 2023 period, credential harvesting had fallen from 53% in the September-December 2022 period to just 16%.

The most likely explanation for the consistent decline in reporting of generalized credential harvesting is that RH-ISAC member analysts are 1) increasingly reporting more diverse threats, such as specific vulnerabilities and Artificial Intelligence (AI), and 2) increasingly conducting more in-depth investigations into credential harvesting activity and reporting more specifically, such as "Microsoft," to denote that the threat activity is targeting specific vendor credentials.

Microsoft rose from 7% to 16% to tie for first place with Phishing. General ransomware rose from 5% to 13% to the second most reported threat. Third place went to Cl0p (11%), which did not rank in previous lists. Notably, prior top threats such as Business Email Compromise (BEC) at 3%, OneNote (2%), and ChatGPT (3%) did not make the current list, being replaced by threats such as MoveIT (7%), general vulnerabilities (6%), and AI at 4%.



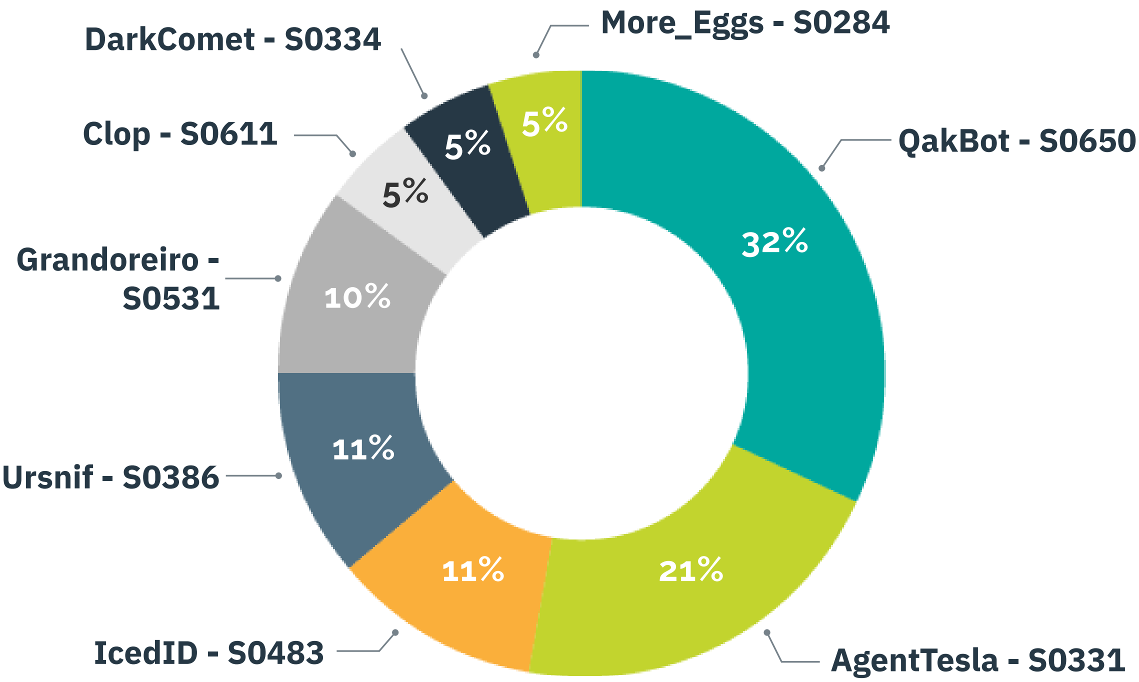
Top MISP Trends

After the launch of MISP by RH-ISAC, threat trends are tracked via the RH-ISAC MISP instance, which changed the way data is presented for threat trends in the Intelligence Trends Summary, beginning with the prior entry for January-April 2023. Tracked data on member-reported threat trends includes prevalent malware, threat actors, intrusion sets, MITRE ATT&CK Techniques, and attribute types.

Top Reported Malware

The top reported malware (MITRE ATT&CK-defined software) by total count of instances, were:

- Cobalt Strike - S0154 (102)
- QakBot - S0650 (6)
- Agent Tesla - S0331 (4)
- Grandoreiro - S0531 (2)
- IcedID - S0483 (2)
- Ursnif - S0386 (2)
- Clop - S0611 (1)
- DarkComet - S0334 (1)
- More_eggs - S0284 (1)

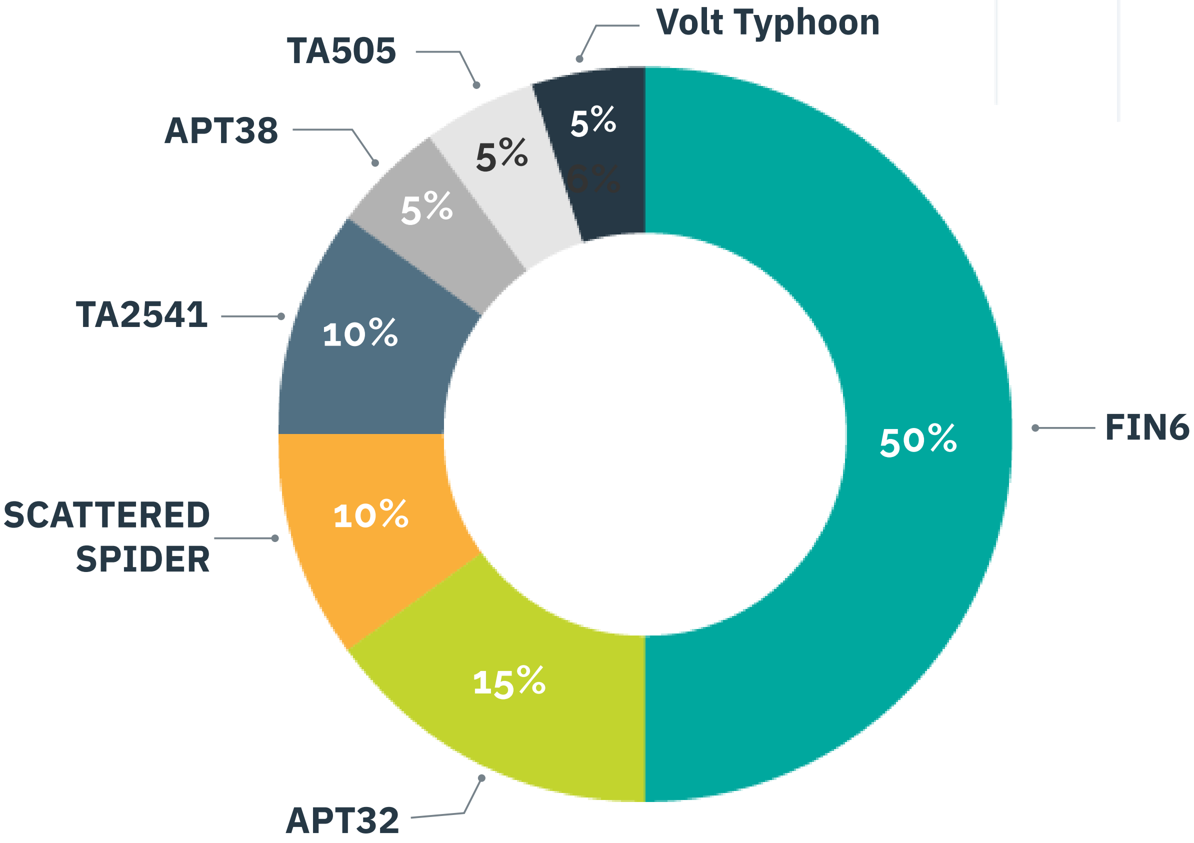


Note: Nearly all Cobalt Strike reporting is from a single source, and is thus not included in the above graph to avoid skewing the perception of the data.

Threat Actors and Intrusion Sets

The top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) by total count of instances were:

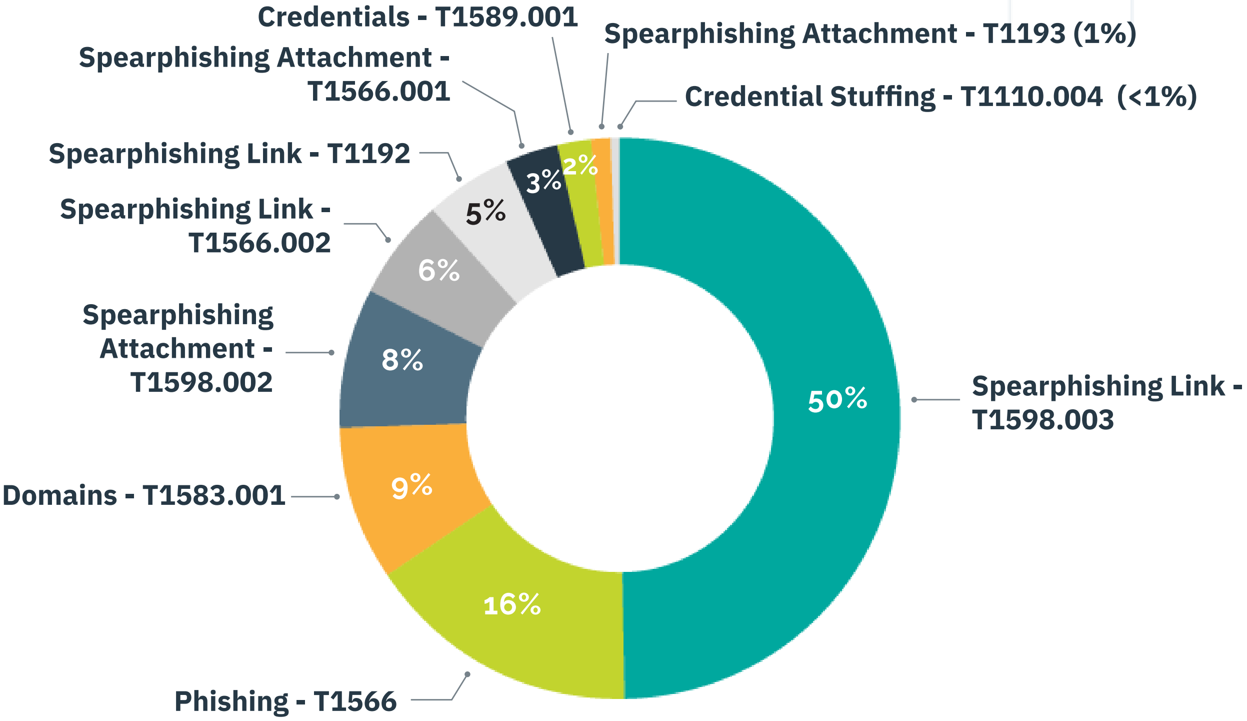
- FIN6 (10)
- APT32 (3)
- SCATTERED SPIDER (2)
- TA2541 (2)
- APT38 (1)
- TA505 (1)
- Volt Typhoon (1)



Top 10 MITRE ATT&CK Techniques

The top reported MITRE ATT&CK techniques by total count of instances were:

- Spearphishing Link - T1598.003 (219)
- Phishing - T1566 (70)
- Domains - T1583.001 (38)
- Spearphishing Attachment - T1598.002 (36)
- Spearphishing Link - T1566.002 (24)
- Spearphishing Link - T1192 (20)
- Spearphishing Attachment - T1566.001 (15)
- Credentials - T1589.001 (9)
- Spearphishing Attachment - T1193 (5)
- Credential Stuffing - T1110.004 (2)

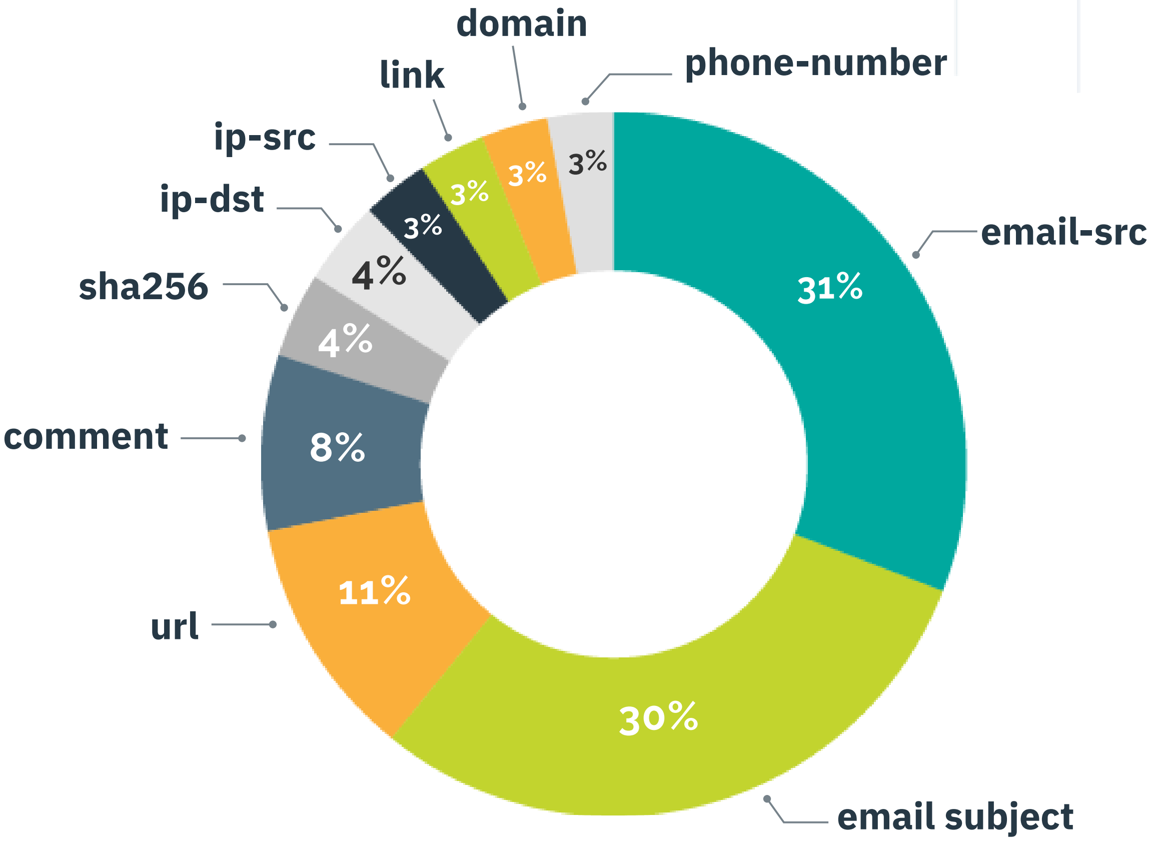


Note: Spearphishing Link and Spearphishing Attachment are presented here twice because they represent identical MITRE TTPs that occur at different stages of the killchain and are thus tracked separately.

Top 10 Attribute Types

The top reported attribute types (categories of technical intelligence shared by members) by total count of instances were:

- email-src- (2289)
- email-subject (2200)
- url (777)
- comment (587)
- sha256 (288)
- ip-dst (266)
- ip-src (250)
- link (248)
- domain (239)
- phone-number (209)



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.

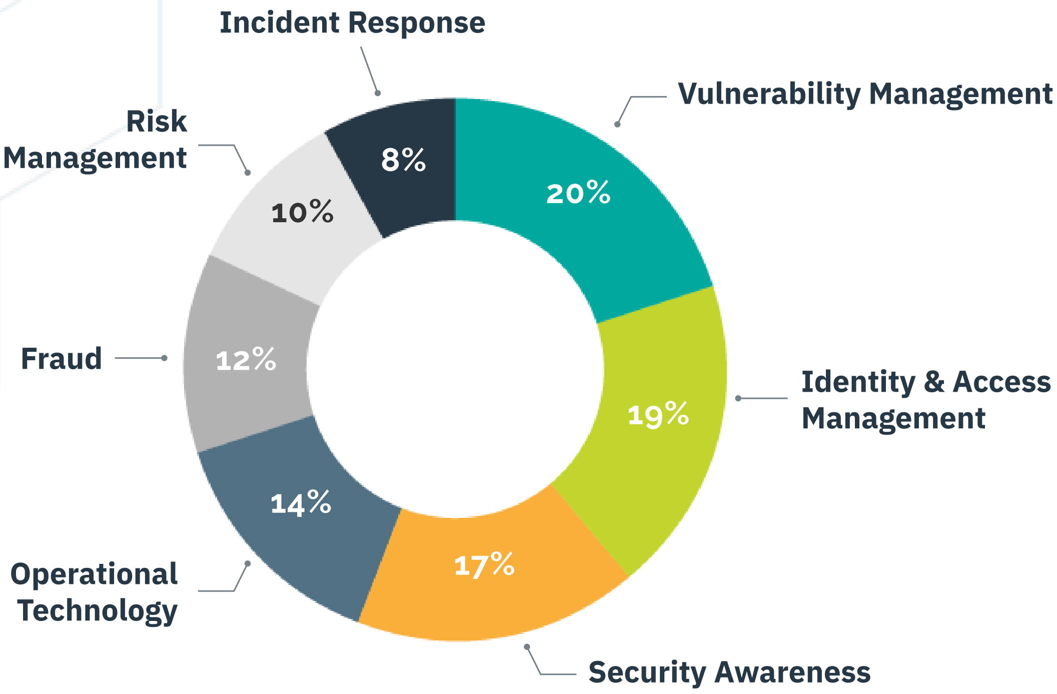
RH-ISAC has continued to track RFIs and surveys to determine what our members are most interested in, from the analyst perspective to the CISOs. Between May and August 2023, 143 unique members, or 57% of our total membership, participated in RFIs or surveys, indicating an interest in crowdsourcing information from peers within the same sector.

In total, for the timeframe of May to August 2023, 119 RFIs were submitted, with 322 responses. In addition, two domain-related surveys were conducted during a similar timeframe that generated 31 responses. The CISO Benchmark Survey is currently live until the end of October.

The figure below displays the category of RFIs, and surveys submitted for January-August 2023.

Top RFI Domains for May - August 2023

119 RFIs | 322 Responses | Average Response: 3



Community Engagement Outlook

In 2022 for the timeframe of May to August, RH-ISAC received 101 RFIs that generated 284 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 (15%) and responses (12%).

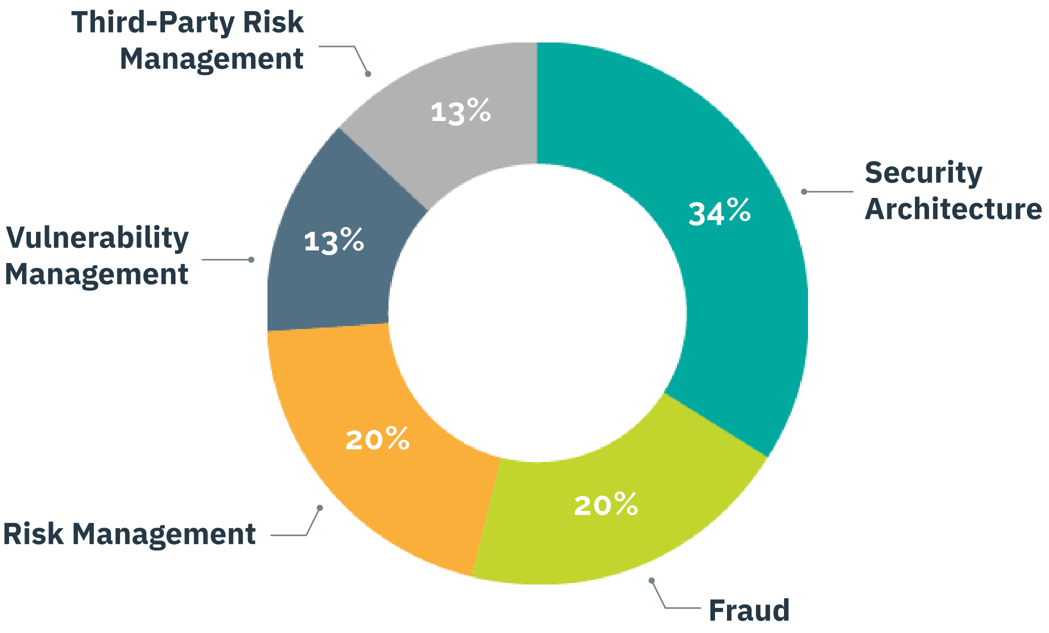
CISO Community Overview

In the CISO Community, for May to August 2023, 17 RFIs were submitted, with 56 responses. During this period, 29% of the RFIs came from the Identity and Access Management Domain with greater interest in sub-domains CIAM, MFA, PAM, and role-based access controls.

Risk Management was responsible for 18% of CISO RFIs with sub-domain topics of cloud governance practices, GRC, Risk Assessment, and Key Risk Indicators. Similarly, Fraud was responsible for 18% of CISO RFIs with sub-domain topics of ATO, phishing, refund-as-a-service, domain takedown, and ransomware.

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

17 RFIs | 56 Responses | Average Response: 3



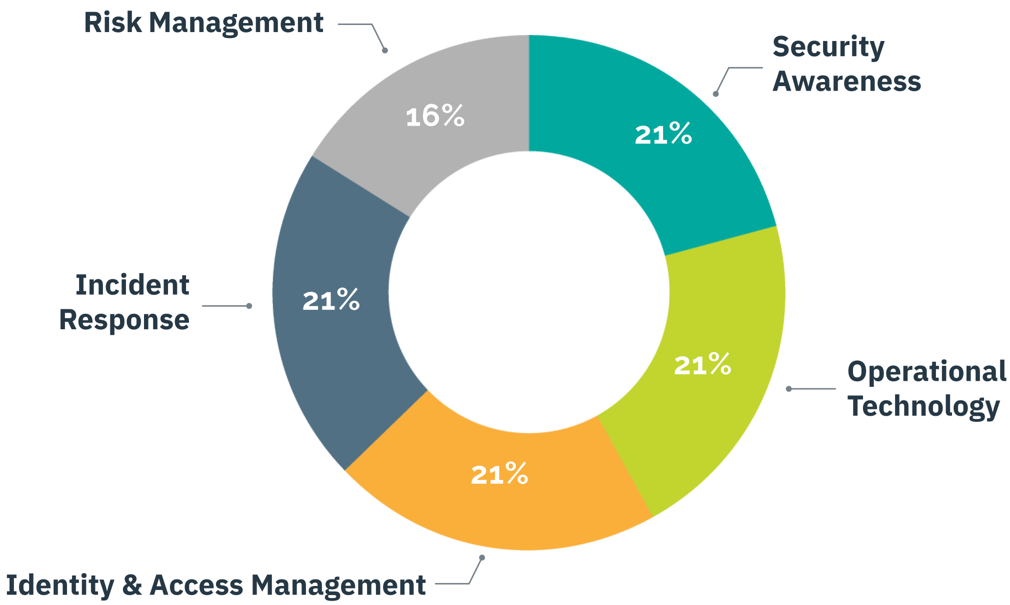
Analyst Community Overview

In the Analyst Community, for May to August 2023, 73 RFIs were submitted, with 170 responses. During this period, security awareness, identity and access management, operational technology, and incident response were key discussion topics among the analyst community, together contributing 22% of overall RFIs.

Like the CISO community, RFIs from the domain identity & access management brought about topics of CIAM, MFA, PAM, and role-based access controls.

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

73 RFIs | 170 Responses | Average Response: 2



Surveys

During May-August 2023, RH-ISAC conducted four surveys and one Benchmark Study.

2023 Cyber Insurance Premium

The purpose of this survey was to determine coverage levels, retention periods, and premium trends. This Survey closed on 5/19/2023 and generated 18 responses.

Protecting Bring Your Own Device

The purpose of this survey was to determine how organizations protect their apps and data on BYOD. This Survey closed on 6/9/2023 and generated 13 responses.

ANALYSIS & INSIGHTS

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.

MOVEit and Cl0p

Context

On June 2, 2023, a zero-day vulnerability, CVE-2023-34362, was reported in the MOVEit Transfer managed file transfer (MFT) solution, which is widely used across multiple industries. There is currently no severity score assigned to the vulnerability. CISA has required all US government agencies to patch the vulnerability immediately.

On June 9, 2023, Progress released an advisory with patches for an additional vulnerability in MOVEit tools, with updates released on June 12, 2023.

On June 5, 2023, the Cl0p ransomware group publicly claimed responsibility for the major reported cyber incidents leveraging CVE-2023-34362. After publicly claiming the exploit on June 5, 2023, Cl0p began posting claimed targets on their dark web blog daily, averaging between 5 and ten claims a day with dates set for publication of stolen data if not paid. Claimed organizations span most industry verticals, including retail, hospitality, and travel.

To date, the organizations claimed by Cl0p in connection to the MOVEit vulnerability that are relevant to the RH-ISAC community include, but are not limited to:

- American Airlines
- Allegiant Air
- Bluefin
- Jack Entertainment
- AMC Theaters
- PayCom
- Discovery
- ShutterFly
- RICOH Acumen
- Agilysys
- Netscout
- RCI

Community Impact

Multiple organizations (including many operating in the retail/hospitality/travel spaces) have been impacted by the zero-day, and Cl0p as a result. Impacted organizations reportedly included the Zellis payroll management company and multiple Zellis customers, such as the British Broadcasting Company and British Airways.

Many of these organizations have supply chain or other business relationships with RH-ISAC members, and all members are encouraged to patch immediately if they use the MOVEit transfer tool in their operations. The RH-ISAC Intel team will continue to provide updates as they emerge.

RH-ISAC Threat Actor Profile Catalog

The Project

In February 2023, the RH-ISAC intelligence team published a catalog of the most prominent and prolific threat groups targeting our community as a resource for member analysts. The catalog 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

Member Input

RH-ISAC is seeking input from the member analyst community, to include any non-public incidents, IOCs, TTPs, or other data that member analysts may have. Member contributions to the threat actor profile catalogue can be attributed to member analysts or anonymous.

Updates and Maintenance

Threat actor profiles will be updated by the RH-ISAC intel team as new data emerges on the groups. New groups will be added to the catalog as necessary, based on their prevalence and threat level to the RH-ISAC community. Members may contribute new data for profiles at any time for inclusion by the intel team.

Current Profiles

To date, the RH-ISAC intelligence team has published six threat actor profiles, with new profiles to be published at a regular cadence moving forward:

- FIN6
- TA505
- FIN7
- Black Basta
- DarkHotel
- SCATTERED SPIDER