Introduction

With 270 member companies from the retail, hospitality, and travel industries, the threat intelligence shared by members of the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is an excellent representation of the trends prevalent in our sector. We wanted to know how our data compared to other sources tracking retail cyber trends. Every year, cybersecurity researchers at Verizon release a Data Breach Investigation Report (DBIR) with an in-depth quantitative analysis of the cyber threat landscape broken down by attack type, region, and industry. Verizon researchers found their retail, accommodation, and manufacturing sectors faced many of the same threats that our members reported: credential stealing, ransomware, and phishing targeting sensitive data for financial gain.

This report compares some of the key takeaways from the Verizon Report with our own member data, providing additional context to help you benchmark your threat landscape against a wider community of your peers.

RH-ISAC member reporting and sharing largely confirms the trends identified by Verizon, with credential harvesting, ransomware, and phishing representing the largest share of threats facing the community. However, RH-ISAC data tracking provides significantly more specific details for the community threat landscape, such as specific malware families targeting members. The advanced capabilities of the RH-ISAC MISP instance also allow us to examine in more granularity the threat actors and tactics, techniques, and procedures facing the RH-ISAC community. Major emerging trends for 2023 across industries included the explosion of vulnerability exploitation in third-party breaches and the adoption of artificial intelligence (AI) by threat actors.