Brand Intelligence

Loyalty Program Fraud

Background

A multinational European hoteling chain sought aid safeguarding a points-based loyalty program that offers a variety of benefits for continued use of the brand's hospitality services.

Challenge

The chain hired Sovereign to support this goal by monitoring and investigating potentially fraudulent actors. Like many global hospitality chains, the company had been a frequent topic of discussion in underground forums, darknet marketplaces, and other black market communities.

Result

Sovereign uncovered a secret online community of cyber criminals who were actively selling, discussing, and distributing illicit access to loyalty program members' accounts, thus allowing the theft of points which could be used to buy room nights or converted to buy airline tickets and e-vouchers from major online retailers. Access to members' accounts also provided access to certain categories of personally identifiable information (PII.) Sovereign identified multiple criminal actors within this community, including one who had illicitly gained access to loyalty club accounts, some with balances of over 100,000 points. We engaged the criminal actor and gleaned key intelligence regarding fraudulent activity threatening the company, including the modus operandi used to compromise the accounts

Insight

In today's global marketplace, the hospitality industry is particularly exposed to complex and ambiguous risks in an increasingly technology-driven world. Loyalty and rewards points programs often walk hand-in-hand with a greater digital footprint, which can also mean greater exposure of sensitive data such as credit card details and other personally identifiable information.

Sovereign Intelligence
1775 Tysons Blvd. 5th Floor
McLean, VA 22102
sovereign.ai