Cyber Intelligence

Card Script Attribution

Background

In 2016, a global European payment processing company engaged Sovereign Reconnaissance to monitor Dark Web and other salient sites for potential extraneous vulnerabilities. With millions of customers and merchants relying upon seamless account access, network continuity is paramount. Identifying trends of cyber criminals hijacking customer login scripts for card-testing would pose a tremendous burden on internal network security, diverting resources, ultimately jeopardizing brand confidence.

Challenge

Two major issues arose once Sovereign Reconnaissance identified original card-testing scripts targeting the company: (1) was the company establishing a reputation as a reliable card testing venue and (2) whether attribution of the culprits was viable?

Result

Sovereign's 24/7 monitoring was deployed with automatic tripwires to capture and index sites posing threats to the client. The tripwire service alerted to the threat of an original card testing script targeting the client's customer identification credentials. Over a dozen profiles were quickly established across multiple internet domains. The detailed profiles were organized by pseudonym, time of postings, ontology, sentiment, motivation, and risk. While those details would have sufficed to demonstrate the growing reputation hazards facing the client, an unusual foreign carding site was discovered, creating the necessity for further *attribution*. Sovereign's forensic team immediately established links between a BitCoin blockchain and a foreign merchant, ultimately providing the site's full transaction details, as well as the merchant's contact information for further fraud notification. Sovereign additionally scanned server banners from the original web server, metadata from the page source, and the Google UID, via our proprietary Reconnaissance search engine, extracting critical information from the foreign ISP. Sovereign ultimately discovered the original ISP and IP of the carding site. The client successfully altered critical components of their network security as a result.

Insight

Alerting multinational transaction companies that card testing is underway only solves part of the problem. Combining Dark Web monitoring with powerful forensic analysis in- house to establish greater understanding of the problem and attribution saves time and resources, directly protecting the integrity of the organization.

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