Executive Summary:

[state of the internet] / security

Volume 6, Issue 3

Loyalty for Sale
Retail and Hospitality Fraud
Criminals aren’t afraid to use our loyalty against us.

As we’ve said before, password reuse is a significant problem in all industries. Loyalty programs have the additional problem with perception. Many consumers don’t think of them as high risk, and are more likely to use weak passwords or mirror passwords across accounts they’re using with another organization. Even if your compromised account isn’t used to book travel or your points aren’t spent on products, the accounts themselves are a valuable product that can be sold to other criminals on the dark web.

When we say “Loyalty for Sale” in this report, we mean it almost literally. While your loyalty to a merchant, airline, or hotel chain might not literally be for sale, there’s a good chance the account associated with a loyalty program you use is.

Jeff Borman, the Founder and Chief of travelINNsights, is our guest author for this edition. He gives us an insider view into the hospitality industry, which is often run by franchisee owners and large branding companies that are working to balance out ROIs while still keeping their own and their customers data safe.

“Twenty years ago, the biggest brands managed hotels; today they manage a customer base. A downside to this ‘asset-light’ approach is that the major hospitality companies rely on the property owners to continue investing in their hotels. Investments range from upgrading the physical property with new furniture designs to hotel management software. When Hilton launched Digital Key in 2016, the first contactless check-in process in the industry, it needed to ensure that every hotel owner installed the proper door locks and executed the proper system procedures. Enhancements like these carry large costs, so a company like Hilton must be very diligent in selecting which initiatives to mandate.”

Jeff Borman, Founder and Chief, travelINNsights

We can’t talk about this without addressing what has really influenced this year – COVID-19 heavily impacted the hospitality and retail industries.

These industries, known for their focus on customer service and face-to-face interaction, either augmented or created several programs to support their customers. However, these measures – including point extensions on various loyalty programs, bonus rewards, etc. – couldn’t stop the drop in business during the first half of 2020.

During the lockdowns in Q1 2020, criminals took advantage of the worldwide situation, circulated password combination lists, and targeted each of the commerce industries. It was during this time that criminals started recirculating old credential lists in an effort to identify new vulnerable accounts, leading to an uptick in sales related to loyalty programs.
Below you can see the logged credential stuffing attacks between July 2018 and June 2020, but we’ve removed one non-commerce customer from the data set because its attack volume generated significant traffic, and only six months of data were available at the time this report was being developed. The first thing to notice is how consistent the attacks are, no matter which line you follow. In the retail, travel, and hospitality industries combined, there were 63,828,642,449 credential stuffing attacks recorded, and more than 100 billion overall. More than 90% of the attacks in the commerce category targeted the retail industry.
Credential stuffing isn’t the only way that criminals target the retail, travel, and hospitality industries. They target organizations in these industries at the source using SQL Injection (SQLi) and Local File Inclusion (LFI) attacks. Between July 2018 and June 2020, Akamai observed 4,375,711,860 web attacks against retail, travel, and hospitality, accounting for 41% of the overall attack volume across all industries. Within this data set, 83% of those web attacks targeted the retail sector.

**Top Web Attack Vectors Targeting Commerce**

*July 2018 – June 2020*
We didn’t forget about Distributed Denial-of-Service (DDoS) attacks in this report. These attacks are something any retailer dreads, because if their online commerce portal collapses under an onslaught of packets and malicious traffic, it could cost them thousands of dollars a second.

Between July 2019 and June 2020, as shown in the figure below, the commerce category faced 125 DDoS attacks – 90% of them against organizations operating in the retail sector, with the remainder in travel and hospitality.
The retail, hospitality, and travel industries are consistently targeted by criminals, because they have access to assets that are easily turned into commodities. These assets could be personal information, financial information, brand-based loyalty programs, or all of them combined.

Some of the top loyalty programs targeted require nothing more than a mobile number and a numeric password, while others rely on easily obtained information as a means of authentication. There is an urgent need for better identity controls and countermeasures to prevent attacks against APIs and server resources.

The constant back-and-forth between defenders in the retail, travel, and hospitality industries and criminals isn’t going away. It’s up to the organizations themselves and their internal teams to sync up and work to stay ahead of the curve.

Read the Full Report

[state of the internet] / security Volume 6, Issue 3
Loyalty for Sale – Retail and Hospitality Fraud

Download now