Success Story

How Flare's Dark Web Monitoring Protected a Grocery Chain's Reputation

Overview

- A North American food retailer has a popular online grocery retail platform, a loyalty program, and pharmacy services that were targeted by malicious actors.
- Threat actors would take control of accounts (account takeover) on the eCommerce platform and resell them on illicit networks, affecting the customer's reputation.
- Flare not only aided in finding the stolen accounts on the dark web but also identifying fraud methods to stop attacks before they happen.

Malicious actors perpetrate account takeover attacks through credential stuffing. If they can successfully connect compromised login information with accounts, they are resold on illicit networks.

Manually monitoring for stolen credentials is incredibly time consuming and difficult to find. Sometimes months can go by before CTI teams detect leaked information. Also, malicious actors can publish then remove information between searches, adding another layer of difficulty tracking this down. This time lag creates an advantage for threat actors.

This success story illustrates how Flare's dark web monitoring simplified the North American grocery chain tracking down stolen login credentials from their loyalty program eCommerce platform. This shifted their cyber strategy from reactive to proactive: from addressing account takeovers to flagging stolen accounts and addressing the issue before threat actors could abuse the stolen credentials.

By monitoring high-risk external threats with Flare, the grocery chain not only monitored and stopped external risks, but also accelerated their risk mitigation efforts.

The Challenge

There are over 10 billion leaked credentials on the dark web and that number grows every day.

According to our research, there's an average of 22% of employees with leaked credentials. Leaked credentials can lead to thousands, even millions of dollars of damage for an organization, not to mention the emotional hardships for victims and how that negatively affects their perception of the company.

The grocery store chain's CTI team investigated threat actors targeting the online grocery retail platform accounts for account takeovers. Malicious actors publish threats, hacks, and stolen data across hundreds of illicit sources, which makes manual monitoring too time-consuming. Threat analysts can only find breaches and stolen sensitive data when they know what they are looking for and specifically search for it. Stolen credentials can take about 327 days to identify.

Threat actors specifically like to target loyalty program accounts, most commonly found in the retail, hospitality, and travel industries because:

- They typically do not have 2FA/MFA
- They are not perceived as accounts that need a lot of protection like a banking account, even if they include payment information.

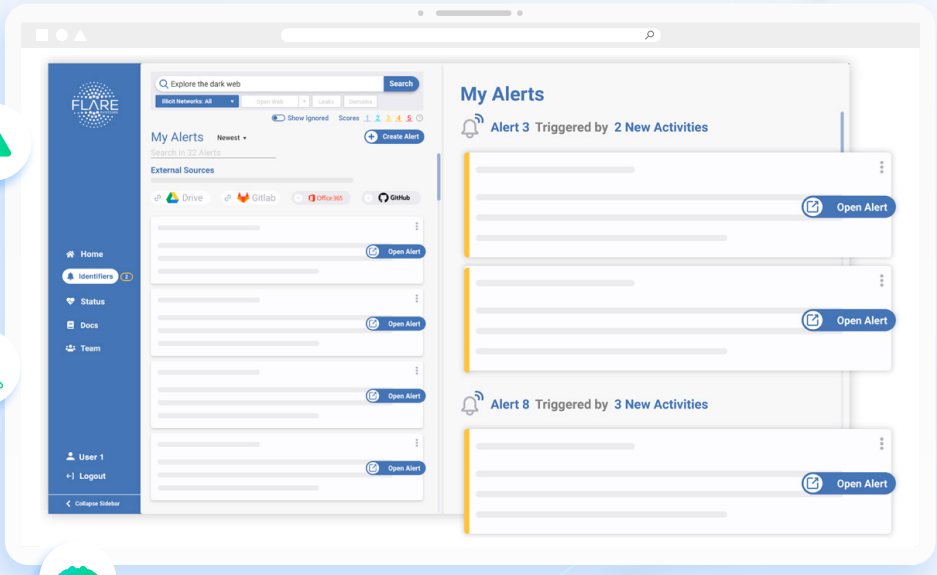
The customer's CTI team looked for technological solutions that would reduce account takeovers and protect the brand reputation while increasing customer retention and loyalty.

Product Highlights

Act on contextualized alerts to **best prioritize** and address threats

Search the dark web **effieciently and safely** in the platform

Identify emerging threats **before** they become attacks



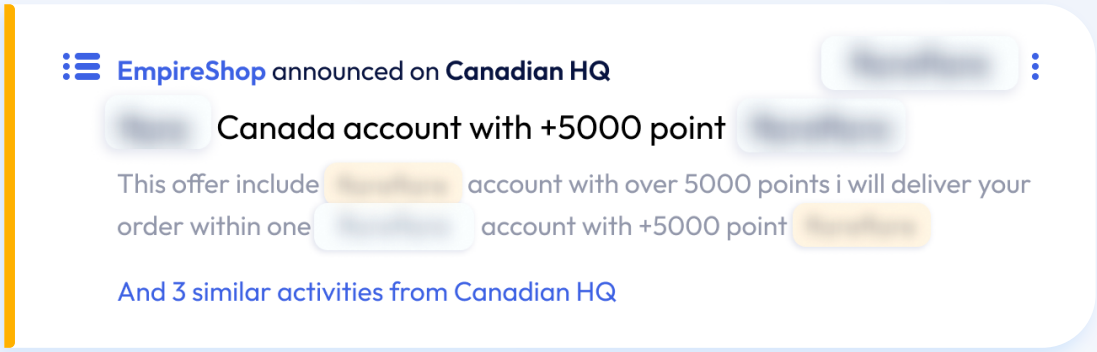
How Flare Helped

A North American grocery chain regained their customers' trust by drastically decreasing account takeovers.

Flare's extensive and automatic dark web coverage enabled the food retailer's CTI team to find stolen accounts and secure them before threat actors gained access through credential stuffing.

The Flare platform provided information on stolen accounts for the customer's CTI team and they quickly flagged those customers' accounts to prevent fraud before it occurred.

By searching through Flare's database of billions of compromised credentials, the customer's CTI team conducted their searches in one place as opposed to combing through hundreds of illicit sources. With this information, they have prevented credential stuffing attacks.



With Flare, the customer could receive alerts within the platform whenever it detected a compromised account.

By monitoring dark web sources where threat actors exchange fraud methods, the CTI team identified critical threats and confirmed that their mitigation strategies were significantly reducing account takeovers and fraud.

Want to prevent fraud before it happens?

Book a demo to learn how we can stop threat actors taking control of accounts before they happen

Book a Demo