

Retail Sector

Source: Deloitte Report



Case 1

Hackers steal card data on millions of customers

Organization

A large retailer that sells a variety of food and non-food products.

Scenario

Attackers installed malware on the retailer's point-of-sale (POS) systems. The infected systems recorded the data for every card swiped through the machine, including PINs. The malware was also capable of spreading itself throughout the organization, eventually infecting millions of POS systems within the retailer and collecting vast amounts of credit card data that was later resold for illicit purposes.

Attackers and motivation

The attackers were identified as organized criminals motivated by the potential financial gain from selling huge amounts of credit card information.

Techniques used

This attack used malware that can be purchased on the criminal market. The attackers installed the malware into the retailer's environment, where it spread itself onto point-of-sale systems that could then be used to extract confidential data and create other backdoors into the retailer's network.

Business impact

The attack received worldwide media coverage, severely damaging the company's brand and cutting into sales. Financial impacts included: a drop in the company's share price over the following quarter and into the next fiscal year; heavy fines; and the cost of offering free credit monitoring to millions of customers.