F500 Retailer Case Study

AUTOMATED GIFT CARD FRAUD

About Shape

Shape Security has deflected over $1B in fraud losses for major retailers, financial institutions, airlines, and government organizations. Shape provides best-in-class cyber-defense against sophisticated automated attacks.

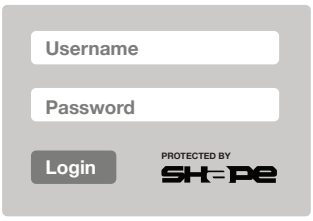
SHAPE

www.shapesecurity.com

Overview

How Shape Defeated Account Hijackers and Saved Tens of Millions of Dollars

A Fortune 500 retailer, manages a gift card program with a stored value of over $5B. Cybercriminals targeted the program, stealing tens of millions of dollars from the company and its customers. Attackers used credentials spilled from other website breaches to hijack customer accounts and steal funds from gift cards. Fraudulent login attempts exceeded a million per day and made up over 90% of the traffic to the login URL. Traditional defenses, like web application firewalls, intrusion detection and prevention services, and fraud analytics, failed to prevent these ongoing automated attacks. The Fortune 500 retailer deployed the Shape solution and completely eliminated account hijackings.

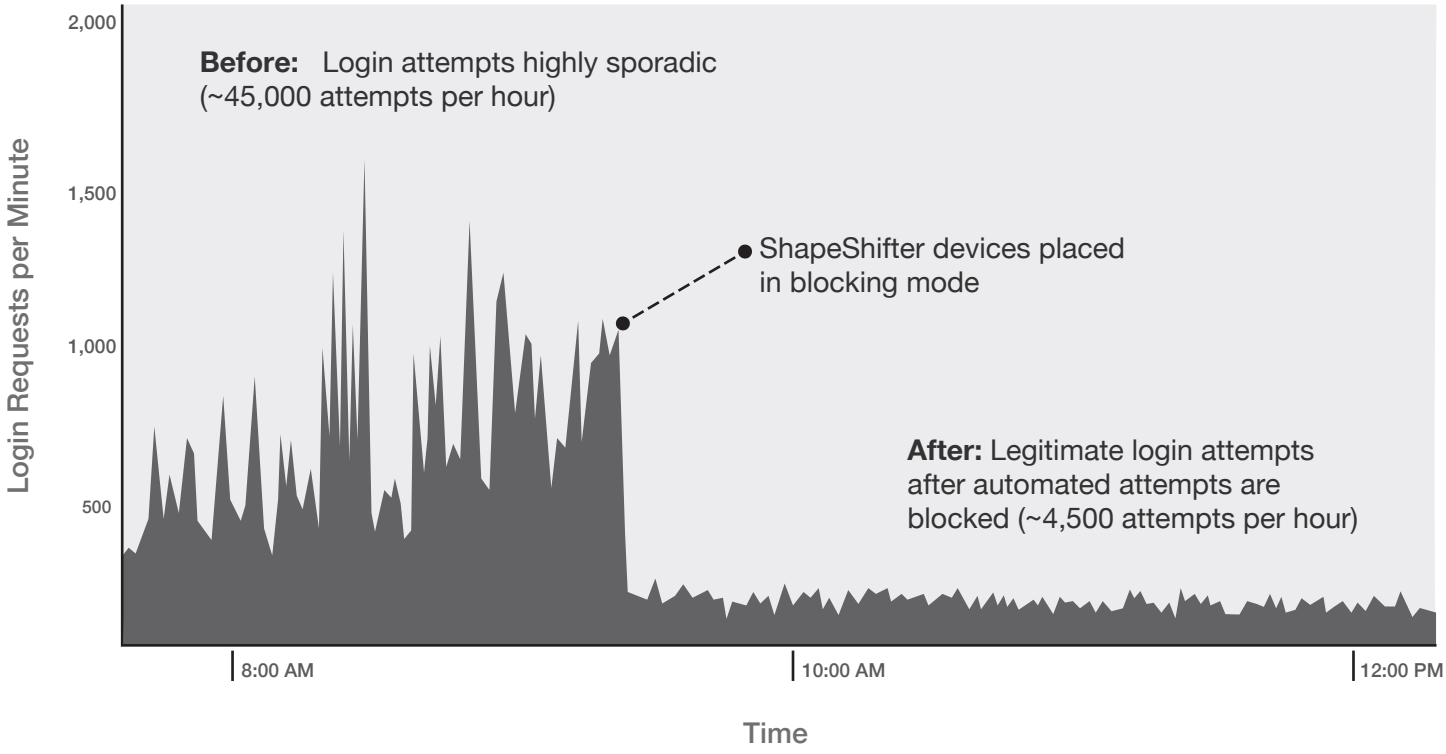


Retailer Description	Fraud & Challenges	Shape Solution
$5B GIFT CARD PROGRAM GLOBAL CONSUMER BRAND	**~1000 ACCOUNTS** HIJACKED PER DAY via credential stuffing attacks	• Eliminated all account hijacking and saved tens of millions of dollars
~20M ACCOUNTS MOSTLY LINKED TO GIFT CARDS & CREDIT CARDS	**BOTS & ACCOUNT CHECKERS** PRIMARY ATTACK TOOLS	• Blocked malicious bots & automated attacks
BALANCE TRANSFERS ALLOWED FROM ONE GIFT CARD TO ANOTHER	**$50** AVERAGE BALANCE OF HIJACKED ACCOUNTS	• Reduced chargeback fees and customer support calls

> *"The problem was with other websites," explained retailer's CISO. "Our customers reuse the same passwords across multiple sites. When other sites get breached, fraudsters use those spilled credentials to hijack my customers' accounts."*

Why Shape?

A Fortune 500 retailer sought out Shape after their WAF, IP reputation feeds, rate limits, and other defensive measures failed to stop credential stuffing attacks. Attackers used botnets, automated account checkers, and web proxies to defeat security measures. At peak, the attacks on the retailer web application involved over 100,000 new IPs that were used once, and never again. Some of the attackers also mimicked browser, or browser agent behavior to simulate human visitor behavior.



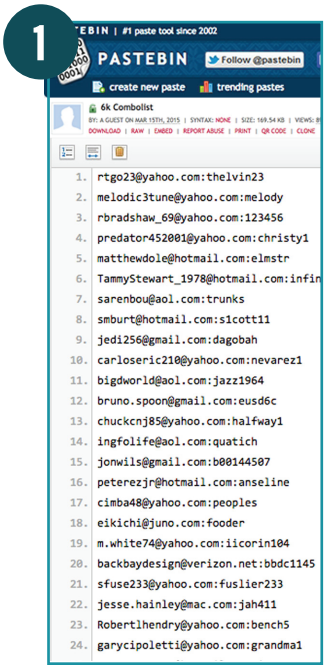
Shape Solution Benefits

- Defended Fortune 500 retailer's website in real-time and successfully deflected automated attacks
- Deployed new countermeasures as attackers adopted different approaches
- Deployed and integrated with retailer's web infrastructure within 2 weeks

> *"The Shape team worked with my team to go live in two weeks from start to finish," explained the retailer's CISO. "Unlike traditional security solutions, we don't need more training or headcount to get value out of Shape's solution. They've completely blocked the attackers without inconveniencing my users or imposing on my team."*

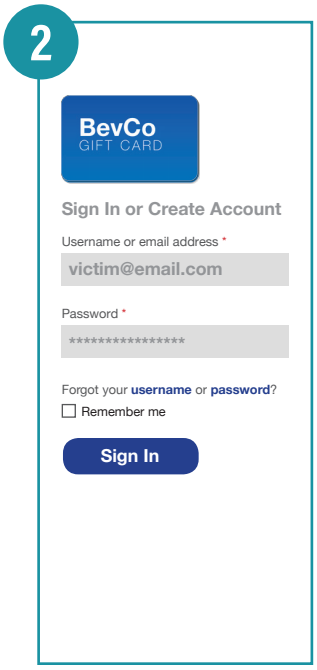
Anatomy of Attack

Automated Account Takeover



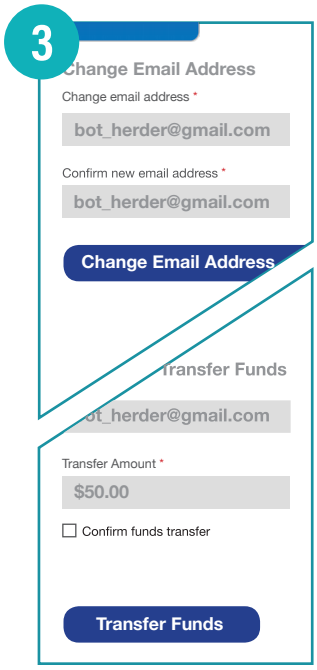
STAGE 1

Attackers acquired spilled credentials from the open web (criminal marketplaces and password dump sites)



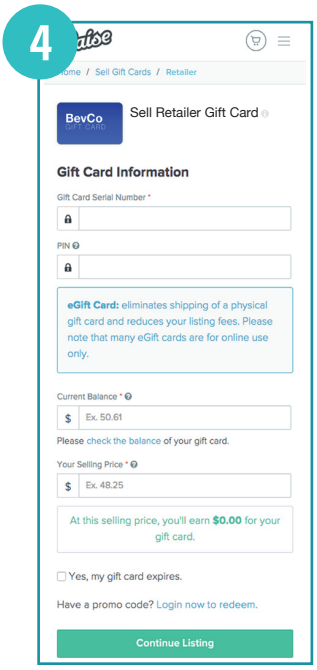
STAGE 2

Attackers tested credentials, using distributed bots, web proxies, and other tactics to evade defenses



STAGE 3

Attackers hijacked accounts when the credentials were valid



STAGE 4

Attackers sold gift cards via secondary markets such as eBay and Raise.com, for 85-90% of their value

Conclusion

Following a successful initial deployment, the Fortune 500 retailer is rolling Shape out to protect additional web applications and API services used by mobile applications. The retailer has eliminated $10s of millions in fraudulent transactions and chargeback fees. The retailer also benefits on an ongoing basis from threat intelligence (collected and correlated across all Shape deployments) and consultation provided by Shape's anti-automation experts to stay ahead of cybercriminals.