CASE STUDY

Automation Gift Card Fraud

RETAILER DESCRIPTION

- **$5B gift card program** global consumer brand
- **~20M accounts** were mostly linked to gift cards and credit cards
- **Balance transfers allowed** from one gift card to another

FRAUD AND CHALLENGES

- **~1,000 accounts** were hijacked per day via credential stuffing attacks
- **Bots and account checkers** were the primary attack tools
- **$50** was the average balance of hijacked accounts

"THE PROBLEM WAS WITH OTHER WEBSITES. OUR CUSTOMERS REUSE THE SAME PASSWORDS ACROSS MULTIPLE SITES. WHEN OTHER SITES GET BREACHED, FRAUDSTERS USE THOSE SPILLED CREDENTIALS TO HIJACK MY CUSTOMERS' ACCOUNTS."

-CISO of retailer

How F5 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 $5 billion. 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 F5® Distributed Cloud Bot Defense and completely eliminated account hijackings.

Distributed Cloud Bot Defense

- Eliminated all account hijacking and saved tens of millions of dollars.
- Blocked malicious bots & automated attacks.
- Reduced chargeback fees and customer support calls.

Why F5?

A Fortune 500 retailer sought out F5 after its 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.

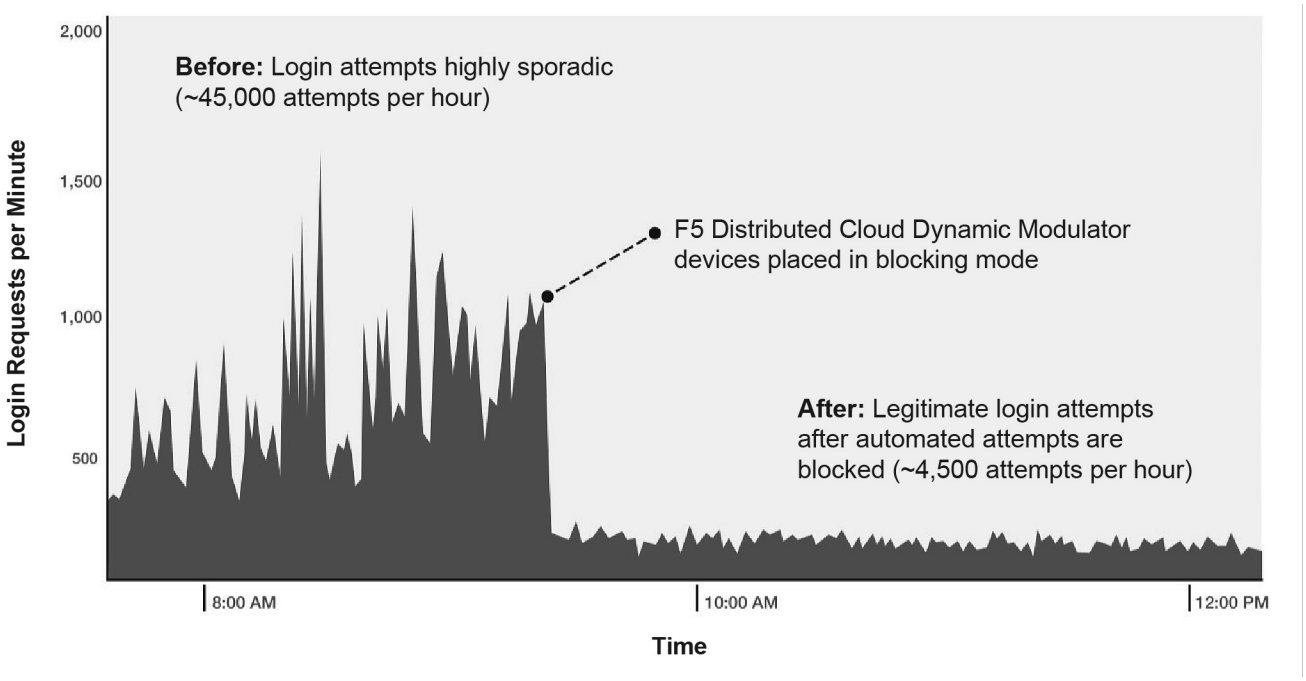


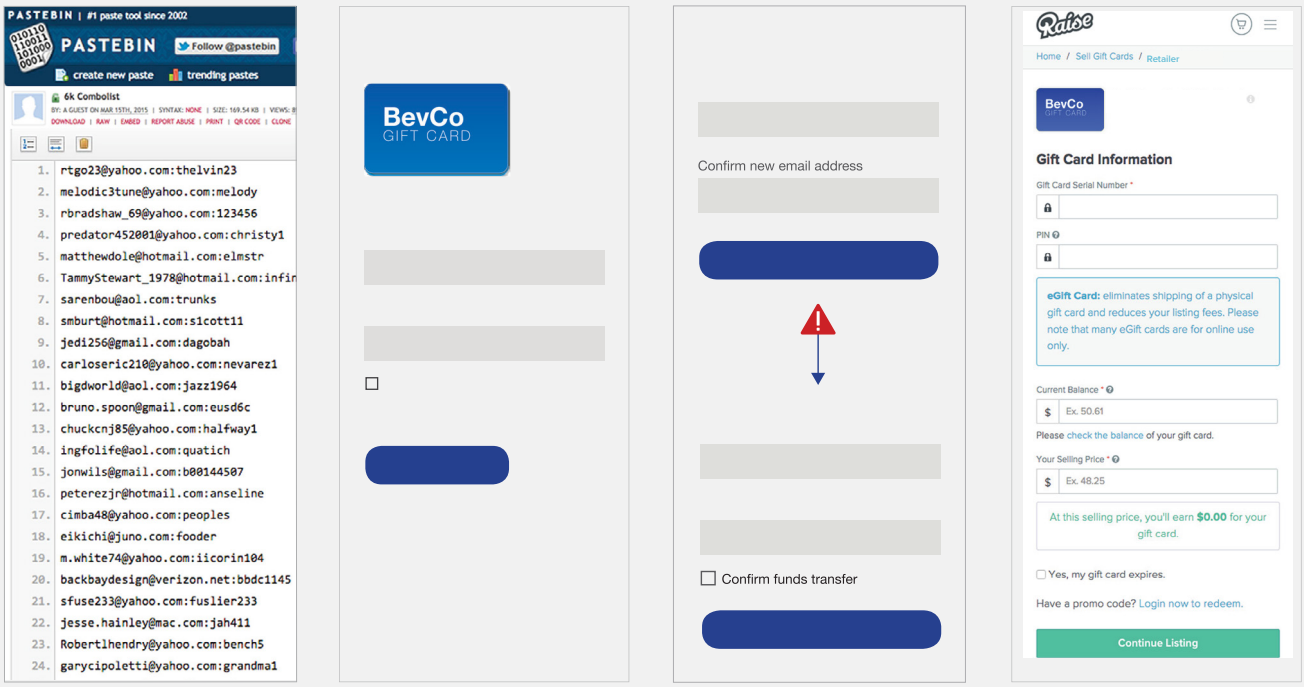
Figure 1: Login requests

"THE F5 TEAM WORKED WITH MY TEAM TO GO LIVE IN TWO WEEKS FROM START TO FINISH. UNLIKE TRADITIONAL SECURITY SOLUTIONS, WE DON'T NEED MORE TRAINING OR HEADCOUNT TO GET VALUE OUT OF F5'S SOLUTION. THEY'VE COMPLETELY BLOCKED THE ATTACKERS WITHOUT INCONVENIENCING MY USERS OR IMPOSING ON MY TEAM."

-CISO of retailer

Distributed Cloud Bot Defense 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 two weeks.



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 defense.

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.

Figure 2: Anatomy of an attack

Conclusion

Following a successful initial deployment, the Fortune 500 retailer is rolling out Distributed Cloud Bot Defense to protect additional web applications and API services used by mobile applications. The retailer has eliminated tens of millions of dollars in fraudulent transactions and chargeback fees. The retailer also benefits on an ongoing basis from threat intelligence (collected and correlated across all F5 deployments) and consultation provided by F5's anti-automation experts to stay ahead of cybercriminals.

To learn more, contact your F5 representative, or visit f5.com.