MEMCYCO

Bank Credential Stuffing
Use Case Analysis

Overview

One of North America's top ten banks faced persistent credential stuffing attacks on its website – without even knowing that. Fraudsters had been using automated tools to input stolen username-password pairs en masse to scale ATO attempts.

Previously, the bank could not detect such attacks, let alone identify affected customers. After deploying Memcyco's breakthrough customer ATO and Fraud Protection solution, that all changed.

Three pillars for next level credential stuffing response

Memcyco's breakthrough tech introduced several transformative anti-fraud capabilities:

- **Seeing attacks-in-progress, not in retrospect**: Memcyco's Customer ATO and Fraud Protection solution flagged in real-time devices that were actively submitting bulk login requests in rapid succession.
- **Getting the '*need-to-know*':** The bank was alerted about attacks-in-progress automatically and near-instantly, helping activate a rapid, targeted insight-led response.
- **Identifying and notifying:** By cross-referencing credentials used in the attack against the customer database, those impacted were quickly identified and notified.

CLIENT CHALLENGES

1. **Credential Stuffing Attacks**
   Automated fraudster submission of login credentials attempting trial-and-error account breaches.
2. **Lack of Real-Time Detection**
   Previously unable to detect such attacks as they occurred.
3. **Attack Forensics Blind Spots**
   Zero way to identify the attack source, or which customers were exposed or impacted.
4. **Powerless to Raise the Alarm**
   Missing attack forensics meant no method for laser-focused comms, to alert the right customers and avoid spooking those unaffected.

Full visibility, ATO security, and insight-rich response

The bank now receives real-time notifications of dozens of credential stuffing attempts daily, allowing them to swiftly act and protect customer accounts.

Further, their security team can now quickly identify and notify impacted customers, thereby reducing the risk of account takeover.

Overall, the improved capability to detect and respond to security threats significantly enhances the bank's cybersecurity posture.

ATO attack risk

SLASHED VIRTUALLY OVERNIGHT

Tactical posture

FROM 'RECOVERY' TO 'PREVENTION'

PR meltdowns

SAFELY AVERTED OR MITIGATED

The bottom line

'Transformative' is a big claim, but that's exactly what Memcyco's solution proved to be here in terms of seriously upgrading the bank's ability to combat credential stuffing attacks effortlessly and continually, which was near impossible with traditional approaches.

Accounts = secured. Customers = reassured. Sophisticated ATO attacks = roadblocked.