CASE STUDY

Protecting Financial Institutions from Brandjacking

The Case of an International Bank, a Memcyco Customer

> *"Our ability to promptly identify customers affected by a brandjacking attack allows us to quickly take action and protect both our customers and us from the negative consequences of the attack."*
>
> **Bank executive**

About the Customer

Memcyco's customer is a multinational financial institution which ranks among the top 500 banks globally. With a notable global outreach, the bank caters to millions of customers worldwide, offering a diverse range of top-notch products and services such as personal and commercial banking, wealth management, and corporate and investment banking.

Business Challenges

A bank under attack

Over the past year, the bank has experienced a concerning increase in brandjacking attacks, with hackers utilizing multiple attack vectors to target the bank's customers including text messages, emails, and phone calls, combined with fake websites impersonating the bank's sites. These attacks have become more sophisticated with time, making it harder for clients to identify the communication as fraudulent. The attackers' tactics included actions such as sending customers links to approve or deny transactions, or to reactivate blocked accounts, by providing login credentials.

Ineffective solutions

Unfortunately, the bank's security solutions, including email scanners, threat intelligence software, and takedown services, have proven to be suboptimal. The bank's team was not aware of the attacks until a customer reported an issue – and the bank only knew about those who complained, leaving the full extent of the damage unknown. Even after taking down an impersonating website, there was always the risk of the same attack occurring from other domains - coupled with the uncertainty of whether all affected users were identified.

Significant damage

As a result of the attacks, the bank incurred unplanned expenses in compensating and benefiting customers who reported issues. Also, a significant amount of time was spent on investigating customer complaints with very little information to go by. The bank also experienced issues in retaining upset customers - and in general suffered reputation damage.

In an effort to prevent further attacks, the bank reduced the number of customer communications through text messages and emails, which negatively affected the bank's efficiency. Although the bank attempted to improve customer education about phishing and impersonation scams, this resulted in customers becoming hesitant and fearful of touching the bank's communications, creating a strain on customer service and account managers. Also, that had a limited impact on helping customers avoid falling into such traps.

Case study at a glance

Customer

A multinational bank

Challenges

- Frequent brandjacking attacks
- Existent solutions not effective
- Financial & reputation damage

Solution – Memcyco PoSA

- Users on fake sites get red alerts
- Alerts sent to bank in real time
- Hassle-free Installation

Benefits

- Brand reputation unharmed
- Reduced financial implications
- Decreased customer churn

Solution

Memcyco proposed the bank its **Proof of Site Authenticity (PoSA)** solution, providing complete real-time protection against brand impersonation.

Quickly distinguish between fake and legit

With PoSA, customers browsing an impersonating website get an immediate red alert confirming that it is fraudulent.

Full visibility

The bank's team receives the alerts about the attacks at the same time that the customers do, ensuring full visibility of the attacker and the attacked customers.

Hassle-free installation

The PoSA solution is agentless, meaning that it doesn't require customers to install any software on their devices or register to any site or service explicitly. Furthermore, the installation process at the bank took only a few hours, and no expert assistance was necessary.

Upcoming functionality planned

In the next phase the bank is planning to activate a unique feature provided by PoSA: a watermark attached to authentic bank websites, identifying them as legitimate. The watermark is different for every user and is identical for any device that the user employs. This way, users can rest assured at all times that they are browsing one of the bank’s genuine websites.

Benefits

The bank subscribed to Memcyco’s service for the following reasons:

Bank reputation and brand equity protection: this is based on PoSA’s ability to counter brand impersonation attacks by detecting them early on, and by providing full visibility into the attacker profile and the identity of the attacked users.

Customer retention: this is achieved by providing red alerts to the users in real time and delivering that ability across all the bank’s portals.

Cost cuttings: the bank can reduce employee time allotted to damage control, as well as decrease funds allocated to user reimbursement, while keeping regulatory exposure at bay.

Summary

This successful detection and prevention of a number of brandjacking attacks demonstrated the effectiveness of the PoSA solution and its ability to protect the bank from potential financial losses and damage to its reputation.