Customer success story

European bank leverages innovative fusion of cybersecurity and fraud prevention to neutralise a multi-layered scam attack

August 2024

Cleafy

Contents

October 2023 marked the onset of a sophisticated, multi-layered fraudulent campaign that **challenged the bank's cybersecurity defenses.**

At a glance

The bank

European 100% digital bank, headquartered in Milan, Italy.

Circa 1.6 million customers

The challenge

A multi-layered scam attack comprising of:

- Bot attacks aimed at sifting through **2.1 million credentials**
- Advanced scam campaign targeting **1,500 users**
- SMS and spoofed calls to **attempt Account Takeovers (ATO)**
- **Deployment of Copybara malware** to commit Device Takeover (DTO) through malicious SMS

The Cleafy advantage

- **Seamless fusion** of fraud management and advanced cybersecurity
- Discovery functionality
- Session and event investigation
- Transaction Risk Analysis
- Device on Call, User Behavioral Analysis, and Transaction Risk Analysis:
  Mobile malware detection
  ASK (Global threat intelligence layer)

Impactful results

100% success rate in stopping fraudulent transaction attempts

€7.5M potential losses prevented

> **The implementation ensures complete transparency within our banking application, integrating seamlessly with our product without impacting the development lifecycle. This integration supports a more agile approach to enhancing the user experience. Additionally, the platform's SaaS model enhances its appeal by enabling continuous cross-intelligence updates directly from Threat Intelligence findings and a network of banks, thereby increasing its overall effectiveness."**

Head of ICT Security
Top European Digital Bank

Introduction

In early 2023, a prominent bank experienced a low volume of scam attempts, primarily limited to occasional impersonation scams via phone calls. However, **October 2023 marked the onset of a sophisticated, multi-layered fraudulent campaign** that challenged the bank's cybersecurity defenses.

Thanks to Cleafy's advanced capabilities, the bank successfully navigated this threat, **safeguarding millions** of euros and preserving **customer trust**.

The challenge

First phase: Large-scale, advanced bot attack to verify data

Second phase: Escalation to impersonation scams

Third phase: Account Takeover (ATO) attack

Fourth phase: Malware attack

First phase: Large-scale, advanced bot attack to verify data

Data has become the new currency for threat actors in sophisticated scam schemes.

In October 2023, the bank encountered an **aggressive bot attack** targeting an application vulnerability during the customer login process. Fraudsters aimed to sift through 2.1 million credentials - obtained from the dark web as part of a 'fraud-as-a-service' package - to identify genuine bank customers.

While the bot processed large datasets in mere seconds to match user credentials, once Cleafy stopped the bot attack, a **smishing campaign** began to keep validating credentials and maximise the number of identified users. Once fraudsters verified these credentials, they attempted to authenticate them on the genuine app from their devices to further validate the data, enabling their use in subsequent phases of the scheme.

Cleafy was pivotal in identifying and responding to this attack. One evening, the bank's anti-fraud team detected unusual activity on a specific URL through Cleafy's monitoring dashboard. Cleafy's real-time analysis accurately gauged the attack's scope, revealing a bot attack originating from **over 100,000 suspicious IP addresses**. Immediate action followed.

Despite the sophisticated bot evading detection by the bank's firewall, Cleafy enabled the anti-fraud team to **swiftly alert the app and perimeter security teams** about the vulnerability in the bank's app. This prompt action led to the creation of a watchlist for users targeted by the bot attack. Thanks to Cleafy's detection and response capabilities, no further credentials could be validated, limiting the fraudsters to validating only 1,500 of the 2.1 million stolen credentials.

Second phase: Escalation to impersonation scams

Following the first phase, the fraudsters turned their efforts to an impersonation scam campaign **targeting the 1,500 users** identified in the initial attack. Using spoofed calls, they mimicked the bank's phone number to deceive customers into performing reversal transactions under the guise of addressing suspicious activities. The bank received dozens of scam reports daily.

During this phase, the team leveraged data from the watchlist of targeted users' behavioural analysis. This comprehensive approach enabled the implementation of rules to create awareness among targeted users and flag suspicious behaviour. These measures successfully **prevented hundreds of scam attempts** before transactions were initiated, significantly limiting potential damage.

The bank also addressed the app's vulnerability by incorporating **Cleafy's on-call indicators** and the aforementioned data, which helped stop further validation and scam attempts. Although 50 customers reached the point of attempting a transaction during a multi-layered scam attack, these attempts were stopped due to **real-time correlation** of all indicators, including transactional indicators such as instant payments involving large sums and descriptions containing phrases like "transaction reversal."

Third phase: Account Takeover (ATO) attack

After the bank resolved the application vulnerability and the scam campaign was disrupted, the attackers changed their tactics. They started using **SMS and spoofed calls** to attempt Account Takeovers (ATO) with the remaining validated credentials. However, Cleafy quickly detected and stopped these attempts. By combining new device enrolment data with information on users targeted by the bot attack and behavioural analysis, the bank was able to **detect and block ATO attempts**, effectively preventing any fraudulent activity.

Fourth phase: Malware attack

The persistent attackers then resorted to deploying Copybara malware to commit Device Takeover (DTO), sending malicious links via SMS to exploit customer devices when clicked. Cleafy's robust defense mechanisms, including mobile malware detection and proactive threat response, effectively blocked these attempts. Cleafy immediately **identified and neutralised infected devices** (of which it found 10), stopping this campaign in its tracks, safeguarding the bank's customers.

> **"Cleafy's platform has enabled a transition from a risk score-centric approach to a fact-based methodology, ensuring greater effectiveness across all scenarios. This shift enhances the accuracy of real-time attack detection from the earliest stages, supporting optimal response strategies and scalable automation—an essential capability in the face of increasingly sophisticated fraud tactics."**

Head of ICT Security
at Top European Digital Bank

Impactful results

Leveraging Cleafy's advanced approach to **proactively prevent fraud**

Cleafy's ensured that all these fraudulent attempts were **blocked with atomic precision.**

Without intervention from the beginning of the attack chain, the **potential fraud could have reached €7.5 million.**

Achieved a 100% success rate in stopping fraudulent transaction attempts, **preventing potential losses of €250,000.**

The Cleafy advantage

Throughout this multi-layered scheme, Cleafy's comprehensive feature set proved invaluable:

Discover functionality: Enabled the creation of monitoring dashboards for real-time application behavior analysis and threat identification.

Session and event investigation: Allowed detailed verification of activities during the bot attack.

Rules engine: Facilitated the automation of watchlists, detection, and response rules, ensuring swift action against identified threats.

Transaction Risk Analysis: Constructed rules to detect and block suspicious transactions effectively.

Device on Call, User Behavioral Analysis, and Transaction Risk Analysis: Blocked scam attempts with high accuracy.

Mobile malware detection: Proactively identified and countered malware threats, including new variants like Copybara.

ASK (Global threat intelligence layer): Provided timely updates on new malware variants, enabling swift response.

Conclusion

By effectively utilising Cleafy's advanced anti-fraud tools, the bank not only mitigated a complex, multi-level fraud campaign but also **reinforced its security infrastructure** against future threats, all without disrupting services for their customers.

This success story underscores the critical role Cleafy plays in empowering financial institutions to safeguard their assets and customers against evolving cyber threats.

Learn more today

To learn more about how we can help you

- **Visit cleafy.com**
- **Email us at info@cleafy.com**

Trusted by leading European and LATAM banks, boasting a 4.9 score on Gartner Peer Reviews.

Gartner peerinsights. ★★★★★ 4.9