jscrambler

How MeDirect protects their source-code with Jscrambler

A case study by Jscrambler

“Jscrambler fulfilled the entire checklist of the application security worries we had”
Chris Portelli - Chief Technology Officer at MeDirect

Introduction

About MeDirect

MeDirect is a pan-European digital banking company headquartered in Malta, with subsidiaries in Belgium and United Kingdom and about to extend the operations within the Netherlands. Founded in 2004, it's now Malta's third-largest banking group regarding total assets. MeDirect focuses on WealthTech and specialized mortgage lending. It offers different tools and services to help customers manage their money from over 850 funds, 400 ETFs, and 3,000 stocks. It's regulated by the Malta Financial Services Authority (MFSA) and supervised by the European Central Bank (ECB).

MeDirect counts over 106,000 customers and is expanding globally. Their vision is to provide a convenient way for people to manage and control their finances. They offer a mobile application that allows their clients to check their balances and investments, conduct financial transactions, and trading.

MeDirect ensures its customer's security by using advanced encryption and monitoring technology. Even though they don't store any personal banking information on the user's phones, MeDirect was searching for a solution to protect their source code against reverse engineering. They met Jscrambler as they searched for a solution to improve their security as a banking company.

Summary

Motivation:

- Obfuscate private code / private API functionality;
- Prevent reverse engineering;

Motivation:

Jscrambler Code Integrity.

- Polymorphic JavaScript obfuscation;
- Built-in protection against reverse-engineering tools;
- Self-defensive capabilities to stop tampering and debugging attempts;

Results:

- Smooth integration;
- Seamless integration with Native;
- Successful mitigation of reverse engineering attempts at runtime;

Challenges

When choosing the best solution to protect their web application, MeDirect prioritized the ease of integration, as well as the effectiveness of protection.

Before implementing Jscrambler's solution, MeDirect's users were able to access the source code and, since it was plain JavaScript, they could easily extract it.

MeDirect was also worried about impacting the performance of their application - they wanted to guarantee that the new security solution would not represent any impact.

Solution

MeDirect was concerned about users accessing their code, which was built with NativeScript. This represented a security risk as their source code could easily be reverse-engineered. MeDirect tried some obfuscation techniques to hide their code but quickly understood that it wasn't enough to ensure its security. Instead, they sought out a **purpose-built solution** that would harden the code while at the same time not impacting the application's performance.

When searching for a security solution, MeDirect discovered Jscrambler through a few technical blog posts about its Code Integrity solution. They focused on the benefits of **polymorphic JavaScript Obfuscation**, which transforms original source code into a new version that is extremely hard to understand and reverse-engineer, while keeping its original functionality. This security layer also includes Jscrambler's **Code Hardening feature**, which provides up-to-date protection against all reverse-engineering tools and techniques.

MeDirect's team used a few mechanisms to **test the threat resistance level and security effectiveness:**

- Penetration Tests;
- Vulnerability Scanning;
- Code Reviews.

This set of mechanisms was used to measure the ability of the code to resist different types of threats, such as code injection, data theft, and unauthorized access.

Results

MeDirect's team encountered no issues when implementing Jscrambler. They started with the base mobile template first and were able to integrate Code Integrity in minutes as it fit easily into their CI/CD pipeline.

Looking back at MeDirect's requirements, the company had an extensive checklist of application security challenges and Jscrambler managed to fulfill their critical needs, by providing **in-depth protection of their app source code.** MeDirect also registered no impact regarding their application performance, something that was an essential requirement.

MeDirect's Version 5.0.0 Release on Android, which had two major introductions, verified a download size improvement of 42%. The first introduction was Jscrambler's Code Integrity, the second was an upgrade from NativeScript 7 to 8. When checking the actual bundle size difference on the same version, MeDirect's team verified that the **reduction in the JavaScript file size was around 44%.**

MeDirect expects to **implement additional Code Integrity features in the future**. Often, customers start with their most pressing use case and iterate from there. MeDirect's team started with the basic obfuscation template but quickly realized the additional value the solution could provide. They have **complete control over how to deploy the features to ensure in-depth protection of their app source code.**

In conclusion, **Code Integrity's multi-layer protection greatly reduced the attack surface of MeDirect's banking application,** making it much harder for attackers to understand the logic behind the app.

About Jscrambler

Jscrambler started in 2010 to solve an important yet overlooked security problem: vulnerability and exposure of client-side web applications. Our security solutions have expanded to include all client-side web apps, from original code to third-party integrations. Organizations can innovate as often as the business demands while we provide continuous protection.

Our software products are developed entirely in-house by experts focused solely on the client-side. We have the most complete and mature solutions for protecting JavaScript-based web apps.

Our customers include the FORTUNE 500, retailers, airlines, banks and other enterprises whose success depends on safely engaging with their customers online. We keep these interactions secure so they can continue to innovate without fear of damaging their revenue source, reputation or regulatory compliance.

If you want to know more about how Jscrambler can help you prevent client-side attacks, don’t hesitate to contact us.

hello@jscrambler.com | +1 650 999 0010