jscrambler / BFI PLAYER

# Protecting the OTT Player of UK's Lead Film & TV Organisation

CASE STUDY

*"It was very quick to get going with Jscrambler, easy to use, and gave us confidence thanks to the results it produces"*

**Luke Simmons**
Lead Developer of BFI Player

# Overview

## A Reference in The UK

Founded in 1933, the BFI is a registered cultural charity governed by Royal Charter, and the **UK's lead organisation for film, television, and the moving image**. At the very core of BFI is the belief that society needs stories—film, television, and the moving image bring them to life, helping us to connect and understand each other better.

The organisation supports creativity and actively seeks out the next generation of UK storytellers. As part of its mission, BFI grows and cares for the BFI National Archive, the world's largest film, and television archive. They also offer the widest range of UK and international moving image culture through its programmes and festivals - delivered online and in venues.

## Pivoting Film Festivals to Digital

After the pandemic hit the UK in 2020, BFI had to adapt quickly to the new reality. The organisation was preparing the **BFI London Film Festival**, which had to pivot to a hybrid format due to strict Covid restrictions. With the goal of making the programme "the most accessible version of the festival to UK audiences yet", BFI successfully delivered around **50 Virtual Festival Premieres digitally**, providing a rich digital experience to its attendees through BFI Player, their state-of-the-art video player.

# Summary

## CHALLENGES

- Add new security layers to protect the video player's source code
- Harden the code of the client-side watermarking agent
- Prevent content leaks
- Reduce reputational risk
- Deliver secure Web and iOS apps

## SOLUTION

**Jscrambler Code Integrity:**

- Polymorphic JavaScript obfuscation
- Code hardening and runtime protection
- Built-in protection against reverse-engineering and tampering

## RESULTS

- Simple integration and maintenance
- Successfully protected the source code and prevented reverse engineering
- Zero content leaks

# CHALLENGES

One of the biggest challenges BFI faced in this pivot to digital events was the risk of **piracy**. The organisation's festivals are typically the stage for multiple premieres, so delivering these premieres to thousands of different attendees digitally could potentially open the door to **content leaks**.

Both BFI and content rights owners were aware of this risk and so BFI made it a requirement to implement technology that would **maximize the security** of the streamed content. Being a hybrid edition with digital festival premieres, BFI had to ensure there were no security issues that could hurt its reputation.

BFI Player was already geo-restricted to the UK audience. To further securely deliver the exclusive content digitally, the access time was limited for each premiere. On top of that, the organisation needed **client hardening** to protect the player's source code on the client-side.

Additionally, due to the nature of the event, the solution also had to be delivered through a Web app, iOS app, and Chromecast app.

# Solution



*“These were very recent films. Content rights holders required in-depth security, including watermarking and client hardening. We felt safer with that in place.”*

**Margo Cayla**
Product Manager of BFI Player

As part of the organisation’s strategy to mitigate content leaks, BFI implemented Friend MTS’ ASiD OTT Client-composited **watermarking**. This technology applies subscriber-level watermarks to the playback of all available feature films so that any content theft is quickly detected and taken down.

To increase the robustness of this approach, BFI understood the need for a reliable solution that **would protect the watermarking agent** on the client-side and seamlessly integrate into the overall project.

Given Jscrambler’s track record in protecting OTT solutions, and given the mature integration with Friend MTS’ ASiD solution, BFI didn’t hesitate to implement Jscrambler to answer the security demands both from BFI and content rights owners.

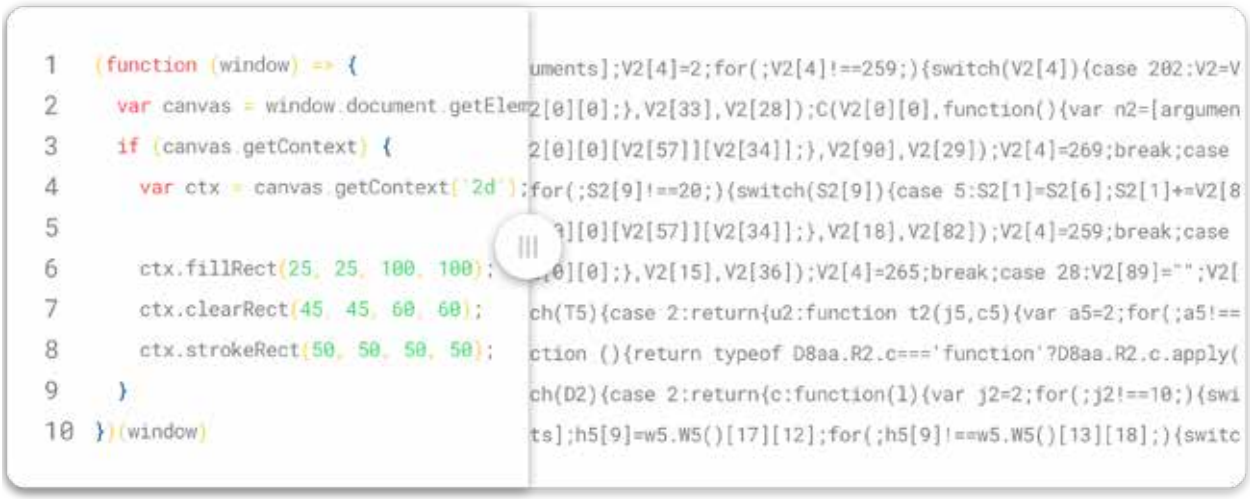
BFI protected the source code of the client-side watermarking agent with Jscrambler’s **polymorphic obfuscation** layer, ensuring that this code was concealed beyond recognition. This obfuscation combines transformations to strings, variables, functions, and objects, through reordering, encoding, splitting, renaming, and logic concealing techniques, to make it extremely hard for attackers to reverse-engineer the code.

# Solution

BFI protected the source code of the client-side watermarking agent with Jscrambler's **polymorphic obfuscation layer**, ensuring that this code was concealed beyond recognition. This obfuscation combines transformations to strings, variables, functions, and objects, through reordering, encoding, splitting, renaming, and logic concealing techniques, to make it **extremely hard** for attackers to reverse-engineer the code.

*"It was one of the simplest decisions we ever made, working with Friend MTS and Jscrambler."*

**Margo Cayla**
Product Manager of BFI Player




Along with this advanced obfuscation, Jscrambler also adds **Code Hardening**, a feature that maximizes the resilience of the protected code, preventing any automated tool from being used in deobfuscation attempts.

Because the video player itself could provide a way for attackers to eventually get to the watermarking agent, BFI also protected the whole source code of the deployed HTML5 player using Jscrambler's obfuscation and code hardening.

With all these protective layers in action, BFI drastically **reduced the attack surface**, making it much harder for attackers to even understand how the software works behind the curtains.

*"We had to deliver not just on the Web, there were also iOS and Chromecast apps."*

**Luke Simmons**
Lead Developer of BFI Player

# Results

Delivering a robust digital experience to tens of thousands of online attendees required BFI to ensure that the security controls would be effective regardless of the device being used.

Jscrambler allowed BFI to **easily protect the code used in all of the required platforms**. Getting started with Jscrambler was a simple process thanks to the **detailed documentation** and Jscrambler's Support team, especially at the initial stages of configuring the product.

Ultimately, the most demanding requirement of ensuring that no attacker could bypass their client-side watermarking agent and leak content was met with success — **there were no content leaks** and the festival went smoothly.

And even though the stakes were very high in premiering high-profile content live online through multiple devices, every stakeholder was very impressed with the results obtained by using Jscrambler to add additional security layers.

*"The documentation was great. Within a few hours, we were obfuscating away using the CLI. It became part of our flow."*

**Luke Simmons**
Lead Developer of BFI Player

# Contact Us

If you want to know more about how Jscrambler can help you secure your media/OTT applications, don't hesitate to contact us

**hello**@jscrambler.com

+1 **650 999 0010**

Gartner®

Jscrambler is the leader in Client-Side Application Security

Recognized in Gartner's **Market Guide for Online Fraud Detection**

and in Gartner's **Market Guide for In-App Protection**

**Trusted by the Fortune 500 and major companies in Finance, Broadcasting, Software Development, E-Commerce, and Healthcare.**