jscrambler

Online video delivery security threats

A data sheet by Jscrambler

OTT video piracy is a growing business threat

As the OTT market is set to double in size by 2024, **piracy is still a key threat to revenue and business sustainability.**

$29B
Online TV and film piracy costs the US economy in lost revenue each year

$12.5B
Expected cost of piracy to pay-TV and OTT providers by 2024

24.5%
Piracy rates for US TV and film will rise from 22% in 2022 to 24.5% by 2027

HTML5/JavaScript power modern OTT platforms

HTML5 and JavaScript brought a faster, more reliable way of delivering online video, but **exposed HTML5 and JavaScript enable attackers to hijack premium content.**

97%
Modern web apps using JavaScript

100%
Fortune 500 companies using JavaScript

150k+
Downloads of free open-source HTML5 video players on GitHub

The threats of exposed HTML5 & JavaScript

Key business threats

Loss of premium content such as live streams, which need to be protected to avoid content hijacking.

Loss of revenue, since attackers can bypass watermarking, re-distribute content, remove ads, or generate fraudulent clicks.

Lack of compliance with content rights owners, as they now mandate OTT providers to ensure that copyrighted content is kept secure.

Loss of customer data including credit card info, user credentials, or personally identifiable information (PII)

Main attacks to OTT platforms

Piracy - Content theft and re-distribution

The HTML5 and JavaScript of video players are exposed, enabling attackers to debug the player and ultimately hijack content. This is especially important in high-value short-duration content like live sports.

Bypassing JavaScript agents like watermarking

Protective solutions such as watermarking often require a client-side JavaScript agent. If this agent is not protected, attackers can easily bypass it or remove it altogether, jeopardizing the content.

Intellectual property theft

Having unprotected HTML5/JavaScript also means that anyone can freely access their source code and potentially uncover proprietary algorithms. Competitive advantages may be at stake.

Data exfiltration

JavaScript is commonly used to create web forms that handle sensitive logic such as credit card data or user credentials. If this JavaScript left is exposed, attackers can tamper with its logic to uncover ways to exfiltrate users' data.

Securing JavaScript/HTML5 in online video delivery platforms

Key business threats

Minimize exposure to piracy by protecting and hardening client-side watermarking solutions and JavaScript/HTML5 streaming players from tampering & bypass.

Enforce licensing agreements by ensuring your code can't be changed by attackers attempting to bypass restrictions.

Protect intellectual property and important algorithms by preventing static & dynamic code analysis.

Code Integrity secures the JavaScript & HTML5 of your web player

Enterprise-grade JavaScript protection

With Jscrambler's polymorphic JavaScript obfuscation and self-defensive capabilities, attackers won't be able to reverse engineer, debug or tamper with your code.

JavaScript code locks

With varying application locks, you can restrict when, where and by whom your web player can be executed (lock by browser, operating system, domain, and date range).

Webpage Integrity protects your web player against malicious modifications

Prevent webpage modification

Attackers won't be able to inject code to modify, remove, or hide features of the web player like client-side watermarking.

Protect sensitive user data by detecting and blocking client-side data leakage attempts in real-time.

Real-time visibility and control

All attempts to inject malicious code or modify the web player's source code will be detected and displayed in full detail on the Jscrambler dashboard. You can choose to block these attacks using fine-grained permission levels.

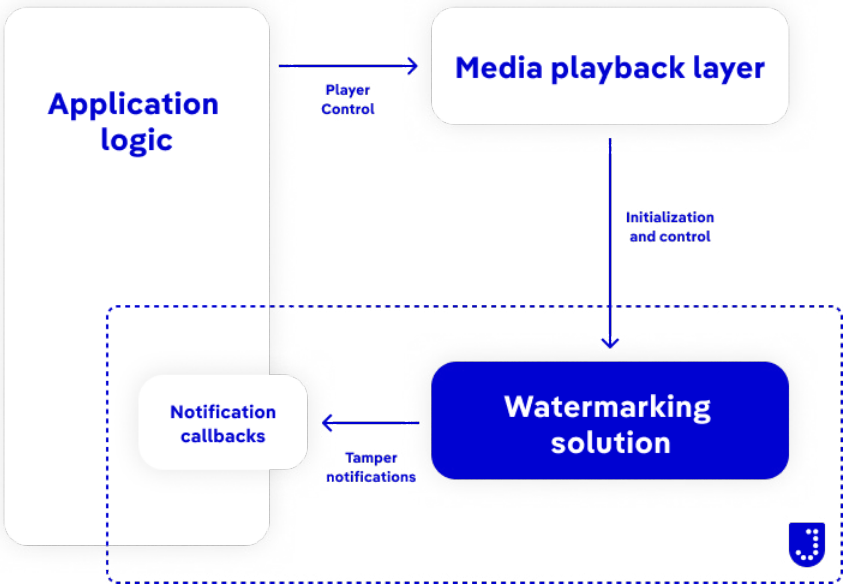
Integrating Jscrambler with watermarking solutions

Jscrambler Code Integrity

- Transforms the code of the client-side JavaScript watermarking agent using advanced polymorphic obfuscation, control flow flattening, and masking/encoding of JavaScript variables, strings, functions, and objects.
- Adds anti-debugging to prevent runtime debugging and using browser developer tools.
- Adds anti-tampering with integrity checks that break the app when ampering occurs.

Jscrambler Webpage Integrity

- Actively monitors the web page for modifications to watermarking client overlays (hide, resize, remove, make transparent);
- Detects changes to the DOM and CSS;
- Detects and blocks malicious extensions and malicious code injections.



References

"Streaming services to lose $113 billion by 2027 due to piracy," by Kyle Fansler, April, 2023, https://www.parksassociates.com/blogs/in-the-news/streaming-services-to-lose--113-billion-by-2027-due-to-piracy

npm Blog, "Managing JavaScript in the Enterprise", February 21st, 2019, https://blog.npmjs.org/post/182958759735/managing-javascript-in-the-enterprise

Download Stats for GitHub, November 2019, https://githubstats0.firebaseapp.com/

Kroll, "2021 Data Breach Outlook", June 2021, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021

Verizon, "2023 Data Breach Investigations Report", https://www.verizon.com/business/resources/reports/dbir/

ImmuniWeb "Abandoned Web Applications: Achilles' Heel of FT 500 Companies", October 24th, 2018, https://www.immuniweb.com/blog/FT500-application-security.html

Ponemon 2022 Study: Data Risk in the Third-Party Ecosystem, https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study

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