Securing Gaming and Business Apps

Game On, for Hackers, Cheaters and Thieves

More than 2.3 billion people play console, mobile, and online video games. According to Newzoo's recent Global Games market report, players will spend about $140 billion in 2018, with more than half of that money coming from the mobile segment. This means that gaming publishers should be worrying about hackers and cheaters—you all know the score. Especially if you look at the number of online sites whose business model is to profit from hacks and cheats.

Then there's the business side of gaming where game companies use web applications to streamline and simplify transactions. However, the client-side code used to enable payments can be an open the door to fraud. Securing web apps against attackers looking to stealing customer credentials and more is no small challenge. To reduce risk and minimize these vulnerabilities, web apps require comprehensive client code protection—to protect customer credentials, payment information and server-side data.

Gaming Apps

The same reverse engineering techniques used to compromise banking apps or other types of ecommerce apps can be used to hack mobile video games. A compromised game app can lead to account takeovers, theft of personal credentials, and/or unwanted access to related payment account or winnings—the same or similar threats that occur when a hacker attacks a business app.

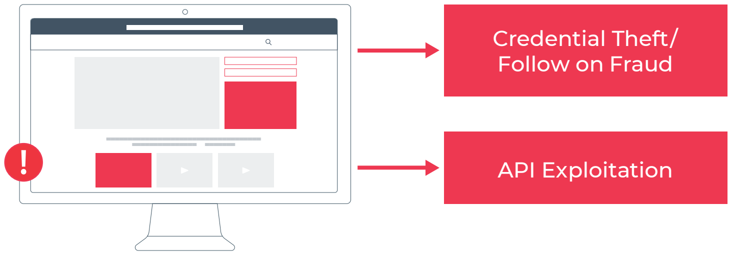
Game Side Reverse Engineering Attacks Enable:

- Game Logic Modification
- Jailbreak Detection Bypass
- IP/Resources Theft
- Texture/Graphic Hacks

Business Web Apps

And from the business side web payment pages are especially vulnerable because about 95% of all websites run JavaScript. As an interpreted language, JavaScript can be easily intercepted, viewed, and compromised since it is sent as text files—unless it is protected—whenever it's used on payment or subscriptions pages.

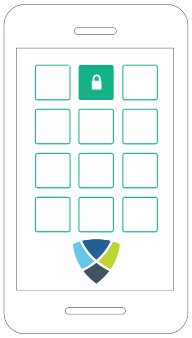
Payment & Subscription Pages



Credential Theft/ Follow on Fraud

API Exploitation

Securing Mobile and Web Apps



Arxan protection stops attacks where they happen because it is integrated at the binary and source code level. This multi-layered approach can automatically be applied to each new revision of code and can easily be integrated into rapid software development lifecycle and DevSecOp environments.

Arxan game protection helps secure mobile, PC, and web app games without disrupting the game development lifecycle:

Game Protection—Integrate game code with a system of code guards and then obfuscate all the code to hide game code and logic to complicate reverse engineering—the root cause that leads to cheating, pirating, and/or app data theft.

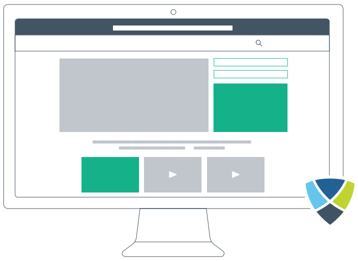
Active Game Defense—Respond to attacks by disabling functionality or shutting the whole game down.

Data and Key Encryption—Hide network keys with White-Box Cryptography to prevent network traffic from being intercepted and critical game data and intellectual property being discovered.

Real-Time Threat Visibility and Analytics—Enable protected games to 'phone home' with vital threat data, allowing teams to stay on top of emerging threats and vulnerabilities.

Jailbreak Detection—Detect high threat environments that are required to efficiently reverse engineer games, along with automation software to create fraudulent game accounts.

Arxan can also protect the revenue and subscription side of your gaming business to counter the threats against the webpages your business depends upon to start subscriptions and collect payments. Arxan for Web quickly protects browser-based web apps by securing "open text" JavaScript with secure obfuscation and can detect active threats by detecting debugger based reverse engineering, or HTML page (DOM) attacks and it can easily be integrated into continuous integration and continuous development (CI/CD), and DevSecOPs environments.



Arxan for Web delivers:

- Passive protection through obfuscation to protect "in the clear" JavaScript code from being easily understood
- Active protection to respond to attacks by shutting the browser down, or by repairing attacked code
- Real-time alerting to notify the organization of code tampering or analysis attempts that can enable immediate operational responses like shutting down attacker accounts or updating code protection

About Arxan Technologies

Arxan, the global trusted leader providing the industry's most comprehensive application protection solutions, works with organizations looking to protect applications and to securely deploy and manage business-critical apps to the extended enterprise. Arxan currently protects more than one billion application instances across many industries including financial services, mobile payments, healthcare, automotive, gaming and entertainment. Founded in 2001, the company is headquartered in North America with global offices in EMEA and APAC.

For more information, please visit **www.arxan.com** or **follow @Arxan on Twitter**.