JScrambler can make HTML5-JavaScript applications Self-defend against tampering threats

New version of the application protection service was just released

Porto, Portugal, March 17th, 2014 – Web security company JScrambler announces the release of JScrambler 3.5, the latest version of the App protection service that brings self-defending capabilities to Web and Mobile applications based on HTML5 and JavaScript technologies.

HTML5 and JavaScript are the standard for cross-platform application development. Using these technologies and you can deploy for IOS, Android, Windows Mobile, Windows 8, ChromeOS, FirefoxOS, and of course, for regular web browsers. There is currently no alternative but to develop from scratch a different version for each platform.

But the main pitfall of HTML5/JavaScript is that is sent and stored on the user device as clear text. This means that is pretty much straightforward to access and read the code. This enables anyone to copy it, reuse it to start a competing business, tamper with it, hack it, and distribute versions of it, in some cases containing malware. This may result in three kinds of losses: competition loss, business loss and reputation loss.

To mitigate these problems the only existing technology is using JavaScript obfuscation, which transforms your original code automatically into an incomprehensible form to a human, while at the same time guaranteeing that the original functionality of the code remains intact. JScrambler is an advanced obfuscator, but it goes further. It leverages the obfuscation by installing a number of different traps throughout the code to enforce your license agreement, to prevent tampering and debugging of your code and to control if the code is being executed in the expected environment.

With its new 3.5 release, JScrambler goes even further. *"JScrambler is the first solution to introduce self-defending capabilities to HTML5/JavaScript applications, including Mobile. The application developer submits its code, we process it automatically by transforming the original code and adding logic that makes the application detect tamper attempts, breaking down on purpose, to mitigate the attacks", said Pedro Fortuna, JScrambler's CTO.*

"We're placing bets on various technologies that have potential to disrupt multiple industries. HTML5 plus JavaScript, when applied to gaming allow us to quickly penetrate a good number of mobile platforms. JScrambler provides the security, and they do it extremely well.", said Ben Chong, CEO of MarketJS, a HTML5 gaming platform.

Other new features in this release include the ability to lock your code to a certain browser or platform, and a feature that allows the developer to include in the code JavaScript comments that tell JScrambler to behave differently in certain blocks of code. You might also be interested to know that not only it supports the aforementioned platforms, but it also supports protecting all sorts of JavaScript libraries, such as Node.js, jQuery, Boostrap, and web gaming frameworks.

JScrambler has been around for almost four years, having so far protected around 150 million lines of JavaScript for users in more than 100 countries. JScrambler just got Series A funding, and is now expanding its operations to the US.

Contact Information:

Pedro Fortuna, Co-Founder and CTO
Email: pedro.fortuna@jscrambler.com
Mobile: +351 917 331 552
Twitter: @pedrofortuna - Skype: pedroffortuna