JScrambler 3 to solve the problem of JavaScript being readable by anyone

New version of the JavaScript obfuscation service is released today

Porto, Portugal, April 17th, 2013 – AuditMark announces the release of JScrambler 3, the latest version of the JavaScript obfuscation service that the company believes will play an important role to protect JavaScript-based applications.

JavaScript is sent as clear text to the client-side Browser and is therefore readable by anyone. This creates several risks: the code might get stolen and reused by competitors; intellectual property, in the form of algorithms, might fall on the hands of third parties; the code might be manipulated, to compromise its license or to exploit visible security vulnerabilities in it.

The problem is being aggravated by the increasing success of JavaScript. In the last years, Webpages have evolved into being larger on the client-side, with numerous JavaScript frameworks coming to play such as jQuery, Ember.js, and AngularJS. Thanks to JavaScript, Web applications now have richer and more interactive interfaces and take better advantage of the computational capabilities available in the client computer. There's a rise in the adoption of standards such as HTML5, with a strong investment from the mobile applications world - and Web GL, for gaming. *"We are seeing Desktop Applications being replaced by Web Applications, first from Google launching the ChromeOS and more recently Microsoft enabling Developers to code Windows 8 Metro applications using solely JavaScript. It is also worth mentioning Node.js applications, which took JavaScript to the server-side. All of these changes tell us that the problem is getting wider and bigger - suggesting that now, more than ever, JavaScript is worth protecting."*, says Pedro Fortuna, AuditMark's Co-Founder and CTO.

JavaScript obfuscation is currently the only technique that allows one to protect its JavaScript-based applications. Obfuscation is the process of lowering the quality of the code in terms of readability and maintainability. The goal is to maximize the amount of time an expert engineer would need to understand it, hopefully to the point where it stops making sense to protect the code, like the software becoming obsolete – and to manipulate it. *"Client side JavaScript will always be accessible to customers and competitors to some degree. Having an extra layer of obfuscation in the early days of building out our product gave us peace of mind."* – Aviel Ginzburg from Simply Measured, a JScrambler client.

AuditMark is releasing JScrambler 3 today, the latest version of its JavaScript obfuscation service. If offers protection for standard JavaScript-based Web Applications, Mobile Web Applications, HTML5 Applications and Web games. *"Perhaps the most important new feature is the JScrambler Box, a virtual appliance for Enterprises with strict security requirements that is deployed to the customer premises"* – says Pedro Fortuna, AuditMark Co-Founder and CTO. But this version also introduces a number of new code transformations to optimize the code, changes to the pricing plans, multi-user accounts, and improved client interface and support information.

With this version AuditMark expects JScrambler to standout as the leading JavaScript obfuscation technology. *"So far we've processed around 120 million lines of code and served users from 106 countries around the World. With JScrambler 3, we want to take it to the next level, and establish JScrambler as the standard in JavaScript protection."*, said Pedro Fortuna, AuditMark's Co-Founder and CTO.

Media contact:

Pedro Fortuna

AuditMark CTO, Co-Founder and Owner

Email: pedro.fortuna@jscrambler.com

Mobile: +351 917 331 552

Twitter: @pedrofortuna

Skype: pedroffortuna

Facebook: https://www.facebook.com/pedroffortuna

Gtalk, G+: pedro.fortuna@gmail.com