## Sécurité et Open Source

# Macaron, une porte dérobée pour toutes les applications JavaEEs

Par Philippe Prados, Expert Sécurité chez Atos Origin

Pour contrer efficacement les agissements des pirates il faut avoir la même curiosité, le même goût qu'eux pour les défis consistant à chercher et trouver la vulnérabilité des systèmes. C'est ainsi que Philippe Prados, Expert Sécurité chez Atos Origin, a détecté des failles de sécurité majeures permettant l'installation de portes dérobées pouvant affecter toute application Java. Au travers d'un article détaillé, il nous présente les résultats de ses recherches sur les techniques d'injection de backdoor, les conséquences possibles et les solutions pour y remédier via trois outils réalisés par la société Atos Origin.


### Résumé

Soixante-dix pour cent des attaques viennent de l'intérieur de l'entreprise. L'affaire Kerviel en a fait une démonstration flagrante. Les projets JavaEEs sont très présents dans les entreprises. On peut même avancer que toutes les grandes entreprises ont au moins une application JavaEE. Par manque de temps, de compétences disponibles ou par excès de confiance, il n'est généralement fait aucun audit pour vérifier qu'un développeur malveillant ou qui subit des pressions n'a pas laissé une porte dérobée invisible dans le code. Dans son article, Philippe Prados propose de se mettre à la place d'un développeur Java pour étudier les différentes techniques permettant d'ajouter une porte dérobée à une application JavaEE, sans que cela soit visible par les autres développeurs du projet. Nous avons développé une archive Java qui permet, par sa simple présence dans un projet, d'ouvrir toutes les portes du serveur. Nous étudierons alors les risques et proposerons différentes solutions et outils pour interdire et détecter ce type de code.


### Pour assister à notre conférence le 5 juin 2009, contacter Anne de Beaumont  01 55 91 24 15

Philippe Prados aura l'occasion de présenter la faille de sécurité identifiée, ses conséquences et les solutions proposées par Atos Origin au cours d'une conférence, le 5 juin 2009, lors d'un symposium sécurité (SSTIC) qui se tiendra à Rennes les 3-4 et 5 juin.

Le SSTIC est une conférence francophone sur le thème de la **sécurité de l'information**, ce qui comprend à la fois les vecteurs d'information (comme les systèmes informatiques ou les réseaux) et l'information elle-même (cryptographie ou guerre de l'information). Il se déroulera à **Rennes les 3, 4 et 5 juin 2009**. Le SSTIC rassemble les personnes intéressées par les aspects techniques et scientifiques de la sécurité de l'information. Les sujets y sont traités de manière **approfondie**, **didactique** et **prospective**.
Pour en savoir plus sur ce rendez- vous : http://www.sstic.org/SSTIC09/programme.do#PRADOS

### Les activités Open Source d'Atos Origin

- http://www.fr.atosorigin.com/fr-fr/nos_activites/nos_metiers/integration_de_systemes/technologies_expertise/logiciel_libre_open_source/default.htm

### Les activités Sécurité d'Atos Origin

- http://www.atosorigin.com/en-us/Services/Solutions/Managed_Operations/AtosTM_Information_Security_Solutions/

### Bibliographie P. Prados

"La qualité en C++" et "C++, Java, Smalltalk" chez Eyrolles, plus de 70 articles dans GNU Linux Mag, Programmez, MISC.

**Atos Origin is the Worldwide IT Partner to the Olympic Games 2004-2012**
**Atos Origin est le Partenaire Informatique Mondial des Jeux Olympiques 2004-2012**