



## **WEB 2.0**

*Quels sont les dangers ?*

*Comment protéger efficacement  
son système d'information ?*

## Sujet traité par Pierre-Marc BUREAU, Chercheur en malware chez ESET, LLC



### **Des attaques sur le Web 2.0 se sont renforcées en 2007, comment procèdent les pirates ?**

Le fait que les attaques sur le Web 2.0 se soient renforcées en 2007 est dû en grande partie au rythme avec lequel les entreprises développent leurs applications. Afin de rester compétitives, ces compagnies publient régulièrement de nouvelles fonctionnalités pour leurs sites, souvent sans les tester suffisamment. Les applications mal testées et développées rapidement offrent un terrain fertile aux pirates qui y trouvent plus facilement des failles de sécurité qu'ils peuvent exploiter.

Les techniques d'exploitation d'applications web n'ont pas beaucoup changé au cours de ces dernières années. Les attaquants utilisent souvent des failles de type « *cross-site scripting* » pour injecter du code (souvent du Javascript) dans des pages web. C'est ce type de faille qui a été utilisé par un ver qui s'est propagé sur MySpace en 2005 (<http://namb.la/popular/tech.html>) et, plus récemment, sur Orkut au mois de décembre 2007 ([http://www.theregister.co.uk/2007/12/19/worm\\_hits\\_orkut/](http://www.theregister.co.uk/2007/12/19/worm_hits_orkut/)).

D'un autre côté, nous avons commencé à observer des attaques exploitant des faiblesses de sécurité spécifiques à certains sites utilisant les technologies du Web 2.0. Par exemple, une application malveillante a été distribuée sur le site Facebook dernièrement. Cette application dirigeait les utilisateurs voulant l'installer vers un site web externe à Facebook et tentait d'installer un logiciel espion sur l'ordinateur des visiteurs.

### **Les craintes pour 2008**

Nous pensons que les applications Web 2.0 continueront de gagner en popularité en 2008 et que les attaques dirigées contre celles-ci se renforceront aussi. Ce que nous devons craindre c'est que les attaques passent du stade de « preuve de concept » (comme les vers MySpace et Orkut) et qu'elles deviennent beaucoup plus professionnelles. Comme ce fût le cas avec les logiciels malicieux dans les dernières années, les attaques contre le Web 2.0 risquent d'être motivées par le vol d'information et la recherche de profit.

### **Protéger son système d'information**

La vigilance et l'éducation des utilisateurs restent la meilleure défense contre ce type d'attaque. Comme il est de mise pour les courriers électroniques, les utilisateurs du Web 2.0 ne devraient pas consulter des messages provenant de personnes qu'ils ne connaissent pas.

Plusieurs services Web 2.0 comme MySpace, Facebook et YouTube fournissent rarement un contenu qui est nécessaire au bon travail des employés d'une compagnie. Il pourrait être envisageable d'interdire la consultation de ces sites pendant les heures de bureau afin de diminuer les risques d'attaques.

Finalement, la mise à jour de tous les composants logiciels installés et l'utilisation d'un antivirus à jour offrent une bonne barrière de sécurité contre les attaques utilisant le Web 2.0 pour installer des logiciels malicieux sur les systèmes des visiteurs.

## Les applications AJAX : la faille

Le problème qui survient avec la technologie AJAX est qu'une partie du code de l'application s'exécute sur l'ordinateur client, c'est-à-dire sur un système à qui on ne peut pas faire confiance. L'exécution de code côté client est souhaitable parce qu'elle permet d'augmenter la vitesse de chargement et d'améliorer l'expérience de l'utilisateur. Par contre, si des parties de code critique sont exécutées sur le client, celui-ci peut en altérer le fonctionnement et ainsi accéder à des fonctionnalités qui n'ont pas été envisagées par les programmeurs de l'application.

Prenons l'exemple d'un programme s'exécutant du côté client d'une application AJAX responsable de créer une requête vers une base et d'en interpréter les résultats. Cette application pourrait être modifiée par un attaquant pour demander les informations sur les noms d'utilisateur et mots de passe du système.

Nous n'avons pas recensé beaucoup d'attaques contre les technologies AJAX. Ces attaques sont très ciblées et spécifiques à chaque application.

### ***Le vol d'informations stockées sur les serveurs***

Ce à quoi nous devons nous préparer pour 2008 est le vol d'informations stockées sur les serveurs qui utilisent des applications AJAX. Avec l'adoption croissante de cette technologie, espérons que les techniques de programmation sécuritaire s'amélioreront aussi.

### **Sécuriser les applications AJAX**

Il est possible de sécuriser les applications AJAX en s'assurant que seulement les fonctions d'affichage et de traitement de données sont effectuées sur le côté client. La validation stricte de toutes les informations retournées par la partie client permettra d'éviter beaucoup de problèmes.