

DÉMOCRATIE

ZATAZ CONTRAINT DE SE TAIRE...

29/01/2009 - Ulhume

Article
Article

Il y a quelque mois j'étais tombé sur une belle faille de sécurité : un site qui donnait un accès libre à des données bien sensibles. Flairant le coup casse gueule, j'avais transmis l'information à un spécialiste du genre, Damien Bancal, du site zataz.com.

Ce dernier avait alors mis en branle son protocole d'alerte consistant en tout premier lieu à prévenir l'intéressé, attendre que la faille soit corrigée, puis bien évidemment publier un article sans pour autant citer ses sources. Du journaliste responsable en somme.

L'ensemble de la démarche est généralement bien apprécié par les entreprises car outre le fait que Zataz ne révèle jamais le moindre détail exploitable, le prix modique d'un article nominatif leur évite, à eux et à leurs clients, des préjudices bien plus graves. Malheureusement, chaque règle donne lieu à ses malsaines exceptions et dernièrement Damien en a fait les frais...

L'histoire commence de la même manière que la mienne, par un internaute qui tombe par hasard sur des données disponibles à travers un serveur FTP ouvert aux quatre vents. Et "tomber" est le mot juste car tout ce qu'il a eu à faire, fut de lancer une bête requête sur son moteur de recherche préféré et d'admirer tous ces curieux résultats en libre accès que ce dernier avait indexé.

Une fois prévenue, la société propriétaire du site FTP en question a, comme les autres, fort apprécié le fameux système d'alerte qui lui a permis de corriger ce trou béant. En revanche, mauvaise joueuse, elle a moins bien accepté la publicité de l'article fait par la suite sur sa mésaventure. Encore l'histoire du beurre, de l'argent du beurre et du postérieur rebondi de la belle crémère...

Ainsi, deux mois après la publication, la société a demandé, via le TGI, la destruction de l'article et des données s'y rapportant. Déjà on appréciera le côté très "bio" de la démarche, sachant que je vois mal l'auteur refuser une demande amicale dans le même sens.

Mais le plus "drôle" dans cette histoire est que l'attaque semble basée sur l'audit d'un "expert en sécurité" qui après avoir ausculté les logs du serveur, a diagnostiqué une intrusion maligne utilisant la très vicieuse technique du compte "ANONYMOUS". Un technique de vilain cracker qui aurait ainsi permis à Damien de contourner l'impénétrable sécurité du système. Il s'agit donc d'un piratage, point-barre...

Pour mémoire, j'ai dû croiser au moins deux douzaines de ces "experts en sécurité" dans ma vie. Un seul était vraiment digne de ce titre, les autres étant un vague ramassis d'opportunistes dont la seule compétence se résumait à la lecture assidue d'Hackademy Magazine. Le patron de cette boîte n'a pas dû tirer le bon numéro...

A ce stade, on se dit qu'il n'y a aucune chance qu'un système de justice sain d'esprit, puisse conclure à autre chose qu'une plaisanterie. Et pourtant... c'est bien ce qui est tombé en fin Janvier. Zataz a donc été enjoint à faire disparaître toutes les informations liées à cette histoire ainsi qu'à payer les frais de justice (7200€ so far), en plus de ce qui a été déboursé pour sa défense. Seule "compensation", le juge semble avoir admis que les données étaient bel et bien accessibles du réseau public. En attendant l'ingrate société a, du moins pour l'instant, ce qu'elle voulait... Belle mentalité.

Cette histoire repose une nouvelle fois les problèmes posés par la divulgation d'une découverte de ce genre. Heureusement, Damien semble décidé à continuer et les 7000 prochaines entreprises qui se retrouveront les fesses à l'air sur le net, par bêtise ou par incompetence, peuvent le remercier pour cela.

Mais l'histoire ne se termine malheureusement pas là avec le procès en diffamation cette fois, qui devrait s'ouvrir mi-février prochain.

En attendant, l'aventure coûte des sous, et il serait donc bien chrétien d'apporter quelques deniers pour au moins rétablir la balance financière et permettre au site de continuer à fonctionner. Pour ce faire, vous trouverez les informations nécessaires à la fin de cet article.