

Ils découvrent une faille sur le site du FIC et terminent en garde à vue

Drôle d'ambiance en ouverture de l'édition 2016 du Forum International de la Cybersécurité (FIC), qui se tient les 25 et 26 janvier à Lille. Nos confrères de 01net racontent en effet la mésaventure survenue à deux jeunes entrepreneurs, qui viennent tout juste de créer leur société spécialisée dans les audits de sécurité et la prévention contre la fraude bancaire, **Cesar Security**. Ces derniers ont découvert une faille, assez banale et aujourd'hui corrigée, sur le site du FIC. Cette dernière permet tout de même d'**accéder à la base de données des participants** à l'événement, racontent nos confrères. Evidemment gênant pour un forum qui accueille chaque année le gratin de la cybersécurité.

Les fondateurs de Cesar Security signalent alors la vulnérabilité par téléphone à l'éditeur du site, la Compagnie Européenne d'Intelligence Economique (CEIS), qui co-organise l'événement. Le 14 janvier, ils publient également un tweet mentionnant le problème. Rebelotte le 20 janvier, avec un second mini-message sur le réseau social.

« Nous avons tout perdu »

Le lendemain, les deux entrepreneurs ont la désagréable surprise de voir **débarquer les gendarmes** du Centre de lutte contre les cybercriminalités numériques (C3N), suite à une plainte de CEIS pour « accès frauduleux à un système automatisé de données ». Délit passible de deux ans de prison et 60 000 euros d'amende. « *Nous avons tout perdu : les trois ordinateurs dans notre bureau, un téléphone, un ordinateur personnel et même une PlayStation* », souligne S. Oukas, l'un des deux fondateurs de la startup [interrogé par 01net](#).

[@FIC_fr](#) MERCI!On découvre une faille sur votre site,on propose de vous faire un audit gratuitement,on se retrouve en garde à vue [#FIC](#) [#CEIS](#)

— CesarSecurity (@SecurityCesar) [January 21, 2016](#)

De son côté, CEIS explique que Cesar Security a tenté de monnayer ses services et parle de pratiques « *d'audit sauvage* ». Ce que conteste la startup, qui affirme avoir proposé un audit gratuit.

Lanceurs d'alerte ?

Ce différend entre les deux sociétés intervient alors que l'Assemblée Nationale vient de voter un **amendement visant à protéger les chercheurs découvrant des failles**. Ce texte, qui vient s'insérer dans le projet de loi pour une République numérique, prévoit de leur accorder un statut de lanceur d'alerte – donc une exemption de peine – à condition d'avoir « *immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système* ».

A lire aussi :

[Vente de zero days : une petite entreprise qui ne connaît pas la crise](#)

[Cybersécurité : un RSI sur deux voit son budget augmenter en 2016](#)

Crédit photo : adike / shutterstock