Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

Deux entrepreneurs se retrouvent en garde en vue après avoir trouvé une vulnérabilité dans le site de Forum international de la cybercriminalité (FIC). Ce dernier, en effet, a porté plainte pour accès frauduleux dans un système informatique.

Attention, le métier de chercheur en sécurité n'est pas totalement sans risque, comme viennent de le constater deux jeunes entrepreneurs qui viennent tout juste de créer Cesar Security, une société spécialisée dans les audits de sécurité et la prévention contre la fraude bancaire.

La semaine dernière, ils trouvent une faille sur le site web du Forum International de Cybersécurité (FIC) qui se déroule ce jour à Lille.

Selon eux, la vulnérabilité – désormais corrigée – était assez banale, mais permettait quand même d'accéder à la base de données des participants. Pas terrible pour l'image de marque d'un tel évènement qui accueille chaque année le gratin français en matière de cybersécurité. Les deux hommes veulent faire les choses bien et contactent l'éditeur du site, à savoir la Compagnie Européenne d'Intelligence Stratégique (CEIS), co-organisateur de l'évènement. Parallèlement, ils envoient une alerte sur Twitter.

Ils sont aimablement reçus au téléphone par un consultant en sécurité du CEIS auprès de qui ils détaillent leur trouvaille. Ils lui envoient un rapport technique de la faille avec une proposition de correctif, un accord de confidentialité ainsi qu'un devis pour un audit de sécurité. « Au départ, nous lui avons proposé un audit gratuit, mais il a dit que ce n'était pas un problème, que l'on pouvait lui envoyer un devis chiffré », nous explique S. Oukas, l'un des deux entrepreneurs. Puis, c'est le silence radio, plus aucune nouvelle. Le 20 janvier, ils envoient donc un nouveau tweet, pour « prendre des nouvelles ».

© DR

Le jour suivant, c'est la surprise. A 9h du matin, les gendarmes sur Centre de lutte contre les cybercriminalités numériques (C3N) toquent à leur porte. Ils apprennent que l'éditeur du site a porté plainte pour « accès frauduleux à un système de traitement automatisé de données » (STAD), un délit passible de deux ans d'emprisonnement et d'une amende de 60 000 euros.

Tout le matériel informatique est saisi. « Nous avons tout perdu : les trois ordinateurs dans notre bureau, un téléphone, un ordinateur personnel et même une PlayStation. Nous sommes tombés de très haut. Nous qui pensions que le FIC aurait encouragé une jeune startup, ils nous mettent à genou. Nous avons perdu nos outils de travail, nous ne pouvons plus rien faire », souligne M. Oukas.

Vente forcée ou chevalier blanc ?

De son côté, le CEIS n'a pas la même interprétation des choses. « Cette société nous a bien contactés, mais ce n'était pas désintéressé car elle nous a proposé ses services. Nous ne l'avons jamais autorisé à effectuer cette recherche. C'est de l'audit sauvage », estime Guillaume Tissier, directeur général du CEIS, qui n'a pas apprécié non plus que Cesar Security publie son alerte de sécurité de manière publique sur Twitter, aux yeux de tous. « Au tribunal, le débat tournera certainement autour de cette question, car on peut le voir comme une forme de vente forcée », estime pour sa part Bernard Lamon, avocat.

L'ironie du sort, c'est que cette affaire tombe pile au moment où les députés votent un amendement visant à protéger les lanceurs d'alerte qui trouvent des failles informatiques. Selon le texte, une telle personne sera exempte de peine « si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système ». Ce texte, s'il est adopté au final, pourrait néanmoins jouer en faveur de Cesar Security. « Même si les faits sont antérieurs, le texte sera applicable car il est plus clément », souligne Bernard Lamon.

Réagissez à cet article

Source : *Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes*