

# Vente de failles et d'exploits : le Français Vupen a bien fourni la NSA

Mis à jour le 19/09 à 14h25 avec les commentaires de Chaouki Bekrar, Pdg de Vupen, en bas de texte

La société de Montpellier **Vupen Security** a bien fourni à la NSA les fruits de ses recherches. Rappelons que la société, dirigée par Chaouki Bekrar, est spécialisée dans la découverte de vulnérabilités logicielles et dans l'écriture d'exploits permettant d'en tirer parti avant que ces failles ne soient comblées par les éditeurs des logiciels concernés. C'est la signature de ce même **Chaouki Bekrar** qu'on retrouve en bas d'un [contrat](#) passé avec la NSA en septembre 2012.

D'une durée d'un an, celui-ci prévoit la souscription aux recherches sur le code menées par la société française et l'accès aux exploits que celle-ci développe. Des cyberarmes que la NSA peut mettre à profit pour pénétrer des systèmes et opérer des écoutes. Rappelons que, selon le *Washington Post*, la NSA a dépensé 25 millions de dollars rien que cette année en achats de vulnérabilités.

## Diffuser des exploits : illégal au regard de la loi française

Ce contrat, qu'a du dévoiler la NSA suite à une demande du site spécialisé dans la publication de données publiques Muckrock, a été largement caviardé par l'agence de renseignement avant divulgation. Le montant de la prestation a notamment disparu. Néanmoins, il place Vupen dans une situation embarrassante, en stipulant que la prestation couvre bien les exploits développés par la firme.

Comme nous l'expliquions dans un précédent article (Lire [Prism : le révélateur du lucratif \(et très discret\) business de la vente de failles](#)) centré sur le marché de la vente de vulnérabilités et d'exploits, et se penchant déjà largement sur le cas de Vupen, un article du Code pénal interdit en effet la commercialisation et la diffusion d'exploits.

Cet article du Code pénal (le **323-3-1** inclus via la loi n°2004-575 du 21 juin 2004) statue que « *le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

## L'Europe sur la même ligne

Un texte qui a valu une condamnation de 1 000 euros à un gérant de SARL spécialisée dans la sécurité, qui avait mis à disposition sur son site « *des scripts permettant d'exploiter des failles de sécurité informatique* ». On retrouve ce même principe dans la toute récente **directive européenne 2013/40** (12 août 2013), où l'Europe presse, dans son article 7, les états membres de prendre les « *mesures*

*nécessaires pour ériger en infraction pénale » la diffusion d'exploits.*

Interrogé sur ces questions début septembre, Chaouki Bekrar, qui connaît pourtant bien l'article 323-3-1 pour l'avoir critiqué vertement sur divers forums, a expliqué, dans un e-mail à la rédaction, que son activité était régulée par l'article R226-3 du Code pénal, qui prévoit une autorisation du Premier ministre pour « *la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente* » de certains appareils ou dispositifs techniques dont la liste est précisée dans un [arrêté](#) du 4 juillet 2012. Une version réfutée par **François Coupez**, avocat associé au sein du cabinet Caprioli & Associés, pour qui ce texte inséré dans la LOPSSI s'applique plutôt aux *malwares* permettant la captation de données informatiques.

**Mise à jour :** Suite à la publication de cet article Chaouki Bekrar, Pdg de Vupen, a envoyé un mail à la rédaction expliquant : « *l'arrêt de la cour de cassation interdit uniquement la diffusion – publique – d'un exploit, c'est-à-dire qu'elle interdit le full-disclosure en France. Les publications dans un cadre privée sont autorisées pour permettre aux sociétés et administrations d'acquérir par exemple des outils dédiés à la réalisation de tests d'intrusion.* »

Crédit photo : © drx – Fotolia.com

---

**Voir aussi**

[Quiz Silicon.fr – Crimes et châtements sur Internet](#)