

# Hacker celui qui vous a hacké ? Illégal mais de plus en plus pratiqué

Une entreprise attaquée par des hackers peut-elle riposter, par exemple pour détruire des documents qui lui ont été dérobés ou mettre hors d'état de nuire des serveurs utilisés par ses assaillants ? En théorie interdites, ces pratiques ont néanmoins été employées aux Etats-Unis, confirme [une enquête de Bloomberg](#), qui explique que les entreprises ont recours aux services d'une **nébuleuse de petites sociétés spécialisées**, où l'on retrouve souvent d'anciens experts militaires ou du gouvernement.

Des pratiques de moins en moins tabou qui commencent à inquiéter le FBI. Selon Bloomberg, qui dit s'appuyer sur deux sources, le 'Bureau' mène au moins une enquête sur le sujet, visant à déterminer si des établissements financiers américains ont recruté des hackers pour mettre hors d'usage des serveurs utilisés par l'Iran pour attaquer les sites Web de grandes banques. Une affaire qui remonte à 2012. L'année suivante, lors d'une réunion confidentielle avec le FBI au sujet de cette affaire, un porte-parole de **JPMorgan Chase** avait défendu le droit de contrattaquer, via des filiales étrangères, expliquent nos confrères. La banque affirme aujourd'hui n'avoir engagé aucune action de la sorte.

## Sony Pictures : un révélateur

Président d'un comité sur la sécurité intérieure à la chambre des représentants, le républicain Michael McCaul évoque la « frustration » des entreprises face aux attaques dont elles sont victimes. Et de reconnaître que certaines d'entre elles sont **tentées de mener des actions de représailles**, « sans obtenir l'autorisation préalable » du gouvernement fédéral. « C'est un peu le Far West », ajoute-t-il. Ces derniers mois, de très grandes entreprises américaines ou installées aux Etats-Unis ont été victimes de piratages savamment orchestrés pour leur soutirer des données. Citons pêle-mêle Adobe, [Target](#), [Home Depot](#) ou, tout récemment, [Sony Pictures](#).

Suite au vol de données qu'ont connu ses studios hollywoodiens, rappelons que Sony est [soupçonné d'avoir lancé des attaques par déni de service](#) sur les serveurs exploités par les hackers. Remarquons que quelques jours plus tard, une autre activité du groupe Sony, le réseau de jeu online PlayStation Network, a, à son tour, subi un assaut par DDoS, entraînant une indisponibilité du service.

## RSA : des activités offensives en Israël ?

Aux Etats-Unis, comme en France, **la loi interdit** aux entreprises tout accès non autorisé à une machine tierce. Même pour riposter à une attaque dont elles seraient elles-mêmes les victimes. En raison des dommages collatéraux possibles – les hackers utilisent souvent des serveurs ou PC compromis et non directement leurs propres machines pour lancer leurs attaques -, la pénétration et la désactivation de machines situées à l'étranger sont **vues comme des pratiques très sensibles par l'administration américaine**. Un document dévoilé par Edward Snowden en 2013

révèle ainsi l'existence d'une directive qui fait remonter jusqu'au président des Etats-Unis toute autorisation d'attaque d'un serveur sans l'aval préalable de son pays hôte.

Selon Bloomberg, qui cite une source anonyme, certaines entreprises détournent toutefois la législation américaine, via leurs **implantations à l'étranger**. Ce serait notamment le cas de RSA (la branche sécurité du groupe EMC) qui utiliserait son labo en Israël pour des opérations offensives (Lire [notre récent reportage sur cette activité](#)). L'entreprise, qui n'a pas souhaité commenter ces informations, aurait pris soin d'interdire tout accès à ces activités à ses employés basés sur le sol américain.

**A lire aussi :**

[Vol de données : 2014, année de tous les records \(infographie\)](#)

**Crédit photo : GlebStock / Shutterstock**