Comment le hacker Ochoa s’est-il fait arrêter à cause d’une photo ?

Il y a quelques années Higinio Ochoa fut arrêté par le FBI car il avait piraté différents sites gouvernementaux. Il avait par ailleurs diffusé des adresses et numéros d’officiers de police. Plus connu sous le pseudo “w0rmer”, il était membre de CabinCr3w, apparenté aux Anonymous.

Mais si je vous en parle c’est que la façon dont il s’est fait arrêter est particulière. Plus exactement comment le FBI a réussi à remonter jusqu’à lui. Quelques jours après ses méfaits il twittait l’adresse d’un site web sur lequel on pouvait trouver des données privées justement volées lors des opérations pour lesquelles il a été ensuite arrêté mais aussi une photo de la poitrine de sa petite amie, avec un message juste en dessous sur une feuille.

C’est cette photo qui donnera au FBI des informations déterminantes. Le FBI va en effet récupérer les données EXIF de cette photo prise depuis un iPhone. EXIF signifie ‘Exchangeable Image File‘. C’est un ensemble de données relatives à chaque photo, générées par l’appareil photo lui-même lors de la prise de vue, automatiquement. Ces infos sont stockées dans le fichier image. Parmi ces métadonnées de la photo, figuraient les coordonnées GPS de l’iphone ayant servi à prendre la photo. La police put ainsi très facilement remonter jusqu’à la copine d’Ochoa et donc jusqu’à lui.