# Une attaque via une Clef USB-HID.

C’est quoi une clef USB -- HID ?

HID (human interface device) ou encore interface homme-machine, c’est une clef USB qui replace les frappes claviers.

C’est quoi une attaque HID ?

Un attaque HID consiste à utiliser le protocole USB-HID pour faire croire à l’ordinateur que le périphérique que l’on a branché est bel et bien un clavier.

La clef USB-HID de référence est la clef USB RUBBER DUCKY.
Elle vaut un peu plus de 100 Euros.
Mais on peut en fabriquer une, soit même, pour moins de 10 Euros.
Vous trouvez de nombreux exemples sur internet.
Vous pouvez même un créer une attaque HID avec un Raspberry PI.

Si vous trouvez une clef USB qui semble perdue sur un parking ou bien laissée négligemment sur un bureau ne l’essayez pas.
Car en quelques secondes elle vous vole vos identifiants et vos mots de passe internet ou bien vous installe un RAT.

Comment se protéger de ces attaques ?

Pour se protéger de ces attaques il n’y a pas de solution miracle, il faut juste du bon sens. Il faut bien faire attention à ce que personne ne branche de périphérique USB à sa machine.
Mais surtout : VERROUILLEZ VOTRE POSTE QUAND VOUS LE LAISSEZ SANS SURVEILLANCE

Si non il existe aussi une arnaque qui consiste à offrir (par exemple dans un lieu publique) une recharge USB gratuite pour vos portables et qui en plus de recharger votre portable via par exemple un Raspberry Pi vous envoie des commandes HID sur votre ordinateur ou votre téléphone. Dans ce cas la parade est simple il suffit d’utiliser un câble USB qui ne fait que charger mais n’a pas fils de liaison pour les data.