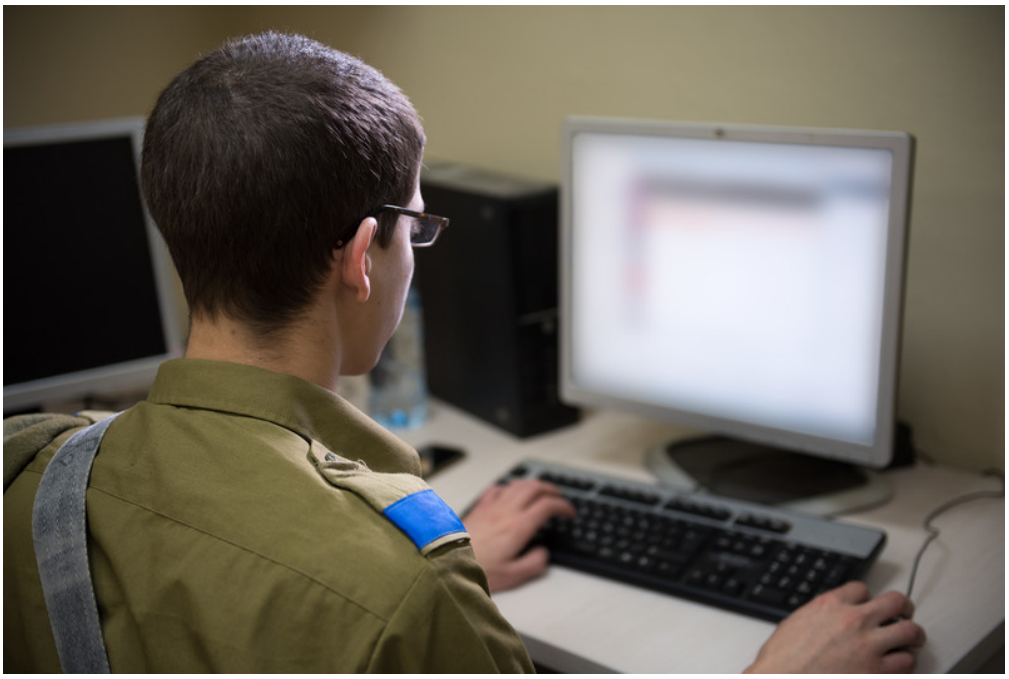
Les espions israéliens volent-ils vos données ?

Katherine Barnett – 5 août 2019



Les diplômés de l'Unité 8200, division technologique de l'armée israélienne, sont impliqués dans de vives controverses sur l'espionnage. (Israeli military/Chameleons Eye/ewscom)

Des espions israéliens
poursuivent des carrières contestables en quittant l'armée.

Des

diplômés de l’Unité 8200 de l’armée israélienne, branche d’espionnage de haute technologie, ont trouvé que deux sociétés de guerre informatique et de collection de données, récemment mises sous surveillance, étaient responsables de l’entraînement de certains des meilleur experts en technologie du pays et des principales actions de la guerre informatique.

La société technologique israélienne Onavo, détenue par Facebook, et la société israélienne de guerre informatique NSO Group ont toutes deux été fondées par des anciens de l’unité.

Ceci prouve combien l’expertise développée dans l’unité peut servir et a servi à créer des plates-formes technologiques commerciales qui mettent la sécurité des consommateurs en danger.

Que fait l’unité militaire ?

L’Unité 8200 est largement considérée comme l’équivalent israélien de l’Agence de Sécurité Nationale aux Etats Unis.

Ses membres sont jeunes, le plus souvent entre 18 et 21 ans, et sont

choisis pour leurs aptitudes en maths, sciences et résolution des
problèmes.

Ceux
qui travaillent dans l'unité aident au développement de la surveillance technologique, du piratage informatique, des techniques
de cryptage et de décryptage. Ils collectent aussi des signaux internes et étrangers et sont responsables de la surveillance informatique et du contrôle des civils.

L'Unité 8200 joue par
ailleurs un rôle significatif dans la discrimination systématique
envers les Palestiniens.

En
2014, 43 réservistes membres de l'Unité 8200 ont révélé des détails sur les méthodes de surveillance utilisées pour fouiner
dans les données les plus personnelles d'innocents Palestiniens,
dont des éléments de nature sexuelle et financière.

« La
population palestinienne sous administration militaire est complètement exposée à l'espionnage et à la surveillance des renseignements israéliens. Alors qu'il y a de sévères limitations à la surveillance des citoyens israéliens, les Palestiniens eux n'ont pas droit à cette protection », ont écrit les soldats dans une lettre publiée dans *The Guardian.*

Malgré la large couverture médiatique qu'elle a reçue, la surveillance des Palestiniens par l'Unité 8200 s'est poursuivie.

L'association militante palestinienne Zamleh a expliqué dans un rapport émis en décembre 2018 comment l'unité intercepte les réseaux de communication palestiniens et y injecte des messages et des appels téléphoniques.

Vol de données

Les anciens de l'Unité 8200 dominent la scène technologique d'Israël. La technologie est la clé de l'économie israélienne et a bénéficié ces derniers temps d'une croissance rapide.

D'anciens soldats de l'unité ont ensuite créé d'importantes sociétés de technologie, dont Palo Alto Networks et Check Point Software Technologies. Ces sociétés se spécialisent dans les questions de sécurité telles que la surveillance, l'enregistrement de voix et la cybersécurité.

Un autre groupe similaire est Onavo, propriété de Facebook.

Cette société a été créée
en 2010 par des diplômés de l'Unité 8200, Rosen et Roi Tiger, et
acquise par Facebook en octobre 2013.

Facebook a mis sur le marché
le réseau virtuel privé (VPN) Onavo en tant qu'outil de confidentialité pour mettre en sécurité les données des usagers
et les protéger de sites internet potentiellement compromis en cryptant et réorientant leurs données via un serveur à distance.

On a laissé les consommateurs
largement dans le noir au sujet des façons dont il violerait leur
vie privée et aiderait à influencer les stratégies de marketing et
de produits de Facebook.

Cependant, l'application VPN
Onavo a été close l'année dernière après qu'on ait réalisé que Facebook payait des adolescents et des adultes pour qu'ils chargent l'application et fournissent un accès « presque sans limite » à leurs données, c'est ce qu'on dit dans la publication *Tech Crunch.*

Après qu'Apple ait interdit
l'application parce qu'elle enfreignait ses lignes directrices,
Facebook a exploité un créneau qui permettrait aux gens de circonvenir la Boutique de l'application et de charger directement

l’application.

Mais, tandis que ceci cachait
tout butinage et activité de l’application aux fournisseurs de l’activité internet, cela permettait à Facebook d’avoir une visibilité presque entière sur les données de l’utilisateur, fournissant à la technologie d’immenses aperçus sur les tendances
de consommation.

Ces aperçus ont conduit
Facebook à décider de mettre en place un article de fond qui lui
permettrait de se mettre en concurrence avec son rival Snapchat. Cela
a aussi permis à Facebook d’acquérir WhasApp pour 19 milliards $
après avoir découvert que deux fois plus de messages partaient de
cette application que de Facebook Messenger.

Commercialisation
de la surveillance

Ce n’est pas la seule fois
où une société liée à l’Unité 8200 a fait l’objet d’un
scandale majeur pour la sécurité des consommateurs.

L’entreprise israélienne d’espionnage NSO Group a été créée en 2010 par Omri Lavie et Shalev Hulio, eux aussi diplômés de l’Unité 8200, d’après *Forbes* magazine.

Ce groupe a fait les grands titres en mai, après que les services de messagerie de WhatsApp aient émis une mise à jour pour lutter contre une vulnérabilité qui permettait que le smartphone de l'utilisateur soit infecté par le logiciel espion Pegasus rien qu'en appelant le téléphone en question.

Une fois que Pegasus est installé sur le téléphone d'un utilisateur, il peut envoyer une quantité effrayante de données à ceux qui pratiquent l'espionnage sans être détectés.

Pegasus a été labellisé par Forbes comme « le kit portable d'espionnage le plus invasif au monde » car il permet la surveillance et le contrôle entiers de tout téléphone portable qui a été infecté.

Ces possibilités ont conduit à son utilisation par des régimes très désireux de fouiner ou d'interférer chez leurs ennemis.

Dans un rapport de 2018, le Ctizen Lab de l'université de Toronto a mis en lumière l'utilisation de la technologie NSO dans des pays connus pour leurs violations des droits de l'Homme, dont Bahrain, le Kazakhstan, le Mexique, le Maroc, l'Arabie Saoudite et les Emirats Arabes

Unis.

Amnesty International a même engagé une action juridique contre le ministère de la Défense d'Israël pour essayer d'obtenir la révocation de l'exportation des produits NSO.

Amnesty a dit que l'un de ses dirigeants était la cible d'une tentative d'espionnage de l'organisation via son personnel.

Que l'Unité 8200 soit derrière l'Onavo de Facebook et NSO soulève des inquiétudes sur le fait qu'une autre technologie commerciale puisse émerger, ou ait déjà émergé, de l'unité d'espionnage.

Avec leur pratique habituelle de la surveillance de masse, il est raisonnable de supposer que les diplômés de l'Unité 8200 continueront d'utiliser cette technologie dans la création de produits commerciaux.

Les activités de NSO et de l'Onavo de Facebook ont montré que les techniques maîtrisées dans l'unité peuvent aisément être dévoyées pour créer des produits qui mettent l'intimité et la sécurité du consommateur en danger.

Les consommateurs devraient donc être au courant de tout lien que les sociétés ont avec

l’Unité 8200, ainsi que de son rôle dans la surveillance des civils.

Katherine Barnett est chercheure pour le site de la revue VPN Top10VPN.com. Ses écrits se concentrent sur la censure mondiale, les droits numériques et la cybersécurité. Twitter : @thekatbarnett.

Traduction : J. Ch. pour l’Agence Média Palestine
Source : The Electronic Intifada