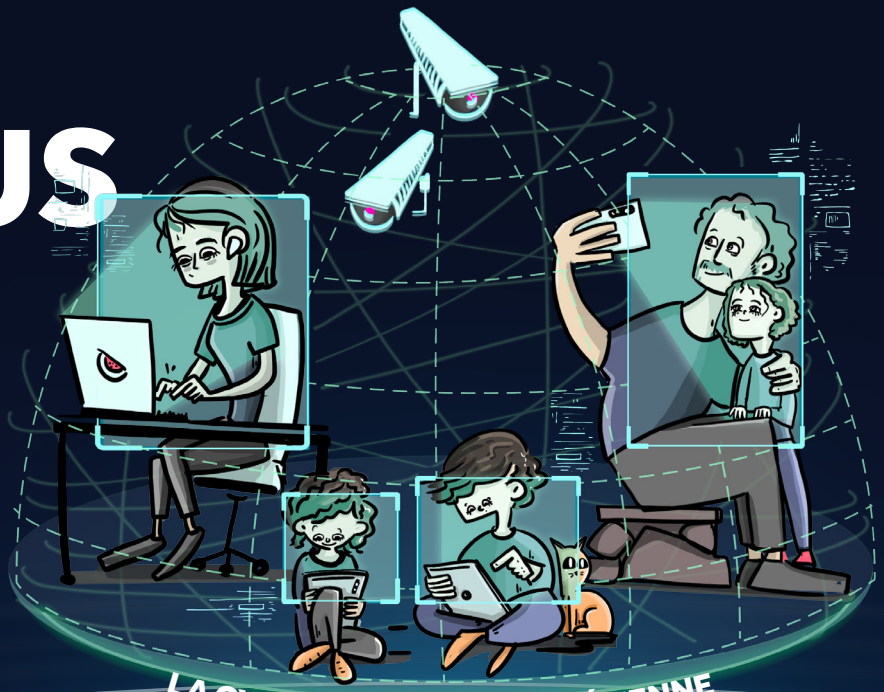
Logiciel espion israélien

Comment s’opposer à un produit qui menace nos droits ?

L'EFFET PEGASUS

L'IMPACT MONDIAL DE LA TECHNOLOGIE DE SURVEILLANCE ISRAÉLIENNE

Les forces militaires israéliennes servent d'incubateur pour le secteur de la surveillance privée du pays : le cas du Groupe NSO, le producteur du logiciel Pegasus, illustre comment des technologies répressives employées sur les Palestiniens sont déployées au niveau mondial. Au moins 45 pays ont détecté des appareils infectés par le logiciel Pegasus.



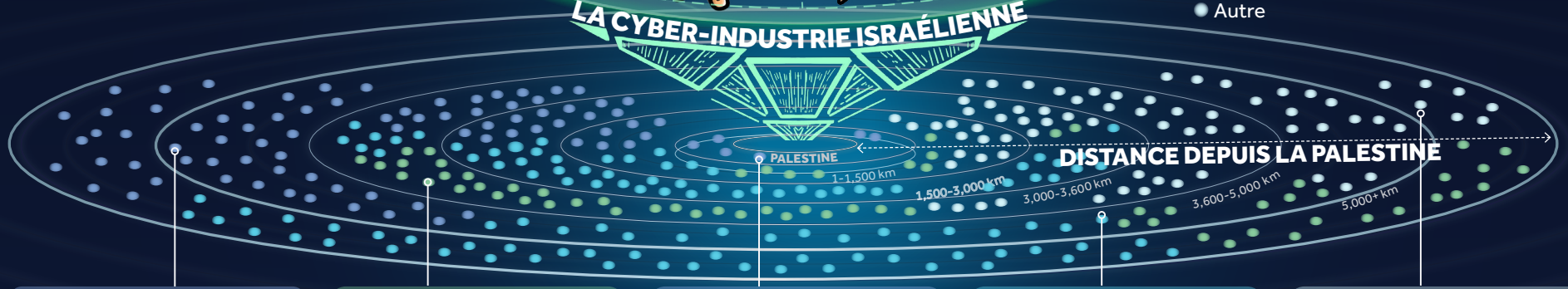
CE VISUEL MONTRE UN PANEL DE

336 INDIVIDUS DE 25 PAYS DIFFÉRENTS

TOUS PRIS POUR CIBLE PAR LE LOGICIEL ESPION PEGASUS EXPORTÉ PAR LE GOUVERNEMENT ISRAÉLIEN.

= 1 PERSONNE INFECTÉE PAR PEGASUS

- Défenseurs des droits humains
- Journaliste
- Homme ou femme politique
- Autre



TOGO
DÉFENSEURS DES DROITS HUMAINS

Un activiste anti-corruption, qui se bat pour une réforme constitutionnelle et électorale, pris pour cible.

ESPAGNE
PERSONNES POLITIQUE

Des dizaines de chefs de file du mouvement indépendantiste catalan pris pour cibles. Le Premier ministre et la ministre de la Défense espagnols ont également été piratés.

PALESTINE
DÉFENSEURS DES DROITS HUMAINS

Des chercheurs en droits humains pris pour cibles. Ils et elles font partie d'associations renommées qui documentent les crimes de guerre Israéliens.

INDE
JOURNALISTE

Des défenseurs des droits humains et des opposants au régime de Modi pris pour cible. Des fausses preuves ont notamment été placées dans leurs appareils.

MEXIQUE
AUTRE

Le parent de l'un des 43 étudiants kidnappes par la police pris pour cible. Les journalistes et les défenseurs des droits humains ont été les cibles les plus fréquentes.

VISUALIZINGPALESTINE AL-HAQ MIND THE GAP

SOURCES https://bit.ly/vp-pegasus
WWW.VISUALIZINGPALESTINE.ORG

@visualizingpal
/visualizing_palestine
fb.me/visualizingpalestine

AUG 2022

Qu'est-ce qu'un logiciel espion (spyware) ?

Les logiciels espions sont une nouvelle technologie d'espionnage. En exploitant les défauts de conception des téléphones et des ordinateurs (connus sous le nom de «zero-day loopholes» — des failles de sécurité inconnues des développeurs), les entreprises privées ont adapté la technologie du renseignement militaire pour espionner les civils. Elles vendent cette technologie aux gouvernements, aux forces de police, aux unités de renseignement et éventuellement à des organisations non gouvernementales telles que des entreprises.

Les logiciels espions ne laissent aucune trace sur les appareils piratés. Ceci permet au client de transformer n'importe quel smartphone en dispositif d'écoute en activant le microphone et la caméra à distance, de lire les documents présents sur le téléphone (y compris l'historique complet de la messagerie, des courriels, des médias sociaux), et même d'écrire du texte et de créer des fichiers qui semblent avoir été créés par le propriétaire du téléphone.

Ces dernières années, les logiciels espions ont été utilisés entre autres contre des militants des droits humains, des journalistes et des avocats, pour faire taire les voix critiques, détruire les partis d'opposition et même orchestrer l'enlèvement, la torture et l'assassinat de personnes. Des preuves de l'utilisation de logiciels espions ont été trouvées dans la tentative de saboter l'enquête sur la disparition de 43 étudiants au Mexique[1] et l'assassinat du journaliste Jamal Khashoggi[2].

Après qu'Amnesty International ait révélé que plus de 50 000 numéros de téléphone[3] ont été transmis à la société israélienne de logiciels espions NSO Group à des fins de piratage, de nombreux experts en technologie — dont l'analyste informatique et lanceur d'alerte Edward Snowden — ont averti que tant que cette technologie ne serait pas interdite[4], elle se répandra facilement et sera utilisée pour cibler des centaines de millions de victimes.

Pourquoi Israël est-il au centre de tout cela ?

Israël est le siège de plus de sociétés de logiciels espions que n'importe quel autre pays du monde[5]. C'est notamment le cas de NICE (cette division de logiciels espions a été rachetée par Elbit Systems, la plus grande société d'armement israélienne), tout comme Verint, NSO Group, Black Cube, Candiru, Cytrox, Cellebrite et Intellexa.

Toutes ces sociétés se vantent du fait que leur technologie provient directement de l'armée israélienne et que leurs fondateurs sont diplômés des unités de renseignement israéliennes «8200»[6], «81»[7] et du Mossad[8].

Cette technologie d'espionnage a été conçue et testée dans le cadre de l'occupation israélienne et du régime d'apartheid en Palestine. Elle a été utilisée pour exercer un chantage sur les Palestiniens pour qu'ils deviennent des collaborateurs. Elle a été utilisée pour saboter le travail des organisations de la société civile palestinienne qui protègent les droits humains des Palestiniens, et pour faire taire les tentatives visant à tenir les forces de sécurité israéliennes responsables des crimes de guerre et des crimes contre l'humanité commis contre les Palestiniens[9].

Une fois la technologie testée avec succès, les sociétés israéliennes de logiciels espions ont été autorisées par le ministère israélien de la Défense à la vendre à des fins lucratives. Elle a été achetée par pas moins de 45 pays, dont des régimes autoritaires et des dirigeants de Biélorussie, du Brésil, du Honduras, de Hong Kong, de la Hongrie, de la Russie, des Émirats arabes unis et de l'Ouganda. De nombreux pays dans le monde ont accès à la technologie des logiciels espions, mais l'État d'Israël la vend activement à des fins lucratives[10].

Pourquoi les logiciels espions sont-ils si dangereux ?

Contrairement aux méthodes de renseignement de la police, les logiciels espions donnent un pouvoir illimité à quiconque les utilise. Il n'y a aucun moyen de procéder à une analyse forensique du téléphone ou de

l'ordinateur infecté pour savoir de quelle manière il a été manipulé. On peut seulement apprendre qu'il a été infecté à un moment donné. Cela permet aux membres des forces de l'ordre qui ont accès à cette technologie de fabriquer des preuves, de recueillir des informations bien au-delà de ce que permet un mandat et d'éviter ainsi de devoir rendre des comptes.

Les fabricants de logiciels espions affirment que leur technologie est destinée à lutter contre le terrorisme et la criminalité, mais il n'existe aucune preuve que l'utilisation de logiciels espions ait permis de prévenir un quelconque crime.

En fait, une fois qu'un logiciel espion a été utilisé contre un suspect, le fait même que les appareils du suspect aient été piratés peut servir de défense pour dire qu'aucune preuve apportée contre le suspect n'est fiable. Les logiciels espions n'aident pas à prévenir le terrorisme et la criminalité, bien au contraire.

Que faut-il faire ?

Les logiciels espions peuvent concerner chacun d'entre nous. Les organisations qui nous protègent de la tyrannie — dans la société civile, dans la représentation juridique, dans les médias — sont toutes vulnérables aux attaques des logiciels espions. Nous devenons vulnérables en tant qu'usagers de la technologie (lorsque nous achetons des téléphones et des ordinateurs) lorsque les entreprises de logiciels espions retournent nos appareils contre nous et violent notre vie privée.

Il incombe à nos gouvernements et à nos institutions législatives et judiciaires de protéger notre sécurité et notre vie privée et d'interdire l'utilisation de logiciels espions. Les fabricants de téléphones doivent être tenus responsables des «zero-day loopholes» (failles du zero-day) plutôt que d'être autorisés à faire des profits, d'abord en les vendant aux sociétés de logiciels espions et ensuite en nous vendant à nous — les clients — des mécanismes de protection ou de nouveaux téléphones pour nous protéger des failles de sécurité qu'ils ont eux-mêmes créées.

Afin d'interdire les logiciels espions, nous devons :

- Construire un mouvement intersectionnel. Nous devons travailler ensemble avec ceux qui ont été attaqués : militants, journalistes, avo cats, défenseurs des droits civils, ceux qui luttent pour la justice clima tique, l'égalité des sexes et les droits des migrants, et ceux qui s'in quiètent du rétrécissement de l'espace démocratique et de la violation de la vie privée.
- Informer le public des dangers des logiciels espions et exiger des actions[11].
- Une simple interdiction ne suffit pas. Des mesures doivent être prises pour garantir que les logiciels espions ne puissent être rentables et que les entreprises qui les produisent et les vendent, ainsi que leurs proprié taires, dirigeants et employés, soient tenus responsables des dom mages qu'ils entraînent

Ensemble, nous lancerons des campagnes sur les médias sociaux, nous ferons honte aux sociétés de logiciels espions et aux entreprises technologiques qui refusent d'assumer la responsabilité des vulnérabilités de type «zero-day» de leurs appareils. Nous finirons par obtenir une interdiction mondiale de cette technologie nuisible.

Nous demandons :

- Une interdiction mondiale de la vente et de l'utilisation des logiciels espions.
- Que les fabricants de téléphones soient tenus responsables, aux niveaux national et international, des failles de type «zero-day».
- Que les fabricants de logiciels espions soient tenus responsables de l'utilisation de leurs produits.

Nous avons l'intention de :

- Construire un mouvement mondial et intersectionnel.
- Mener des campagnes d'information pour sensibiliser le public aux

dangers des logiciels espions.

- Cibler les logiciels espions et les entreprises technologiques qui re fusent de prendre leurs responsabilités.
- Plaider auprès des États, des organisations régionales et mondiales pour qu'ils prennent des mesures visant à interdire les logiciels espions.

Pour des mises à jour régulières, veuillez consulter: **https://bdsmovement.net/israeli-spyware-facilitates-human-rights-violations**

1 https://www.amnesty.org/en/latest/news/2022/08/disappearance-of-43-ayotzinapa-students/
2 https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/
3 https://forbiddenstories.org/about-the-pegasus-project/
4 https://www.inputmag.com/tech/snowden-calls-for-ban-on-spyware-following-nso-group-revelation
5 https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094
6 https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/
7 https://www.haaretz.com/israel-news/tech-news/2021-06-29/ty-article/idf-vs-nso-8200-battle-israel-cyber-talent-getting-dark/0000017f-da7d-d432-a77f-df7f77900000
8 https://www.timesofisrael.com/german-firm-acquires-ex-mossad-chiefs-cybersecurity-startup-for-700m/
9 https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094
10 Ibid.
11 https://www.amnesty.org/en/documents/doc10/4516/2021/en/

BDS
WAR ON WANT
FIGHTING GLOBAL POVERTY
ECCP
European Coordination of Committees and Associations for Palestine
PALESTINAKOMITEEN I NORGE
חרם! מבפנים
BOYCOTT!
From Within
BDS BERLIN
BDS NL
boycot, desinvesteren, sancties
PAN-AFRICAN PALESTINE SOLIDARITY NETWORK
SOUTH AFRICAN BDS COALITION
PSC
BDS India
BDS ITALIA
BDS-CH
Boykott - Desinvestition - Sanktionen
Boycott - Désinvestissement - Sanctions
Boicottaggio - Disinvestimento - Sanzioni
BDS المغرب
BDS FREEDOM JUSTICE EQUALITY
AL-HAQ
TADAMUN