Apple poursuit en justice lâ??entreprise israÃ©lienne dâ??espionnage NSO Group

Description

Par Ali Abunimah, le 24 novembre 2021

Un vendeur palestinien prÃ©sente des produits Apple en novembre 2020 Ã Gaza ville. Apple poursuit en justice NSO Group Ã propos de lâ??utilisation par lâ??entreprise israÃ©lienne dâ??un logiciel espion qui a corrompu des tÃ©lÃ©phones portables dans divers pays Ã travers le monde. (Mahmoud Ajjour / APA images)

Apple est le dernier gÃ©ant de la Silicon Valley Ã poursuivre en justice une cÃ©lÃ¨bre entreprise israÃ©lienne de logiciels espions.

Le fabricant de lâ??iPhone a annoncÃ© mardi quâ??il avait dÃ©posÃ© plainte contre NSO Group et sa sociÃ©tÃ© mÃ¨re Â« pour la tenir pour responsable de la surveillance et du ciblage des utilisateurs dâ??Apple Â».

Apple veut Ã©galement interdire dÃ©finitivement Ã NSO Group dâ??utiliser ses logiciels, services ou dispositifs.

Â« NSO Group et ses clients consacrent les immenses ressources et capacitÃ©s des Ã?tats-nations pour mener des cyberattaques extrÃªmement ciblÃ©es qui leur permettent dâ??accÃ©der aux microphones, camÃ©ras et autres donnÃ©es sensibles sur les dispositifs Apple et AndroÃ¯d Â», a dit Apple mardi.

Â« Des entreprises dâ??espionnage mercenaires comme NSO Group ont facilitÃ© certaines des pires violations des droits de lâ??homme et actes de rÃ©pression transnationale, tout en sâ??enrichissant, elles et leurs investisseurs Â», a dit Ron Deibert, directeur de Citizen Lab [le Labo Citoyen] Ã lâ??universitÃ© de Toronto.

Deibert a applaudi le procÃ¨s et a dit quâ??il espÃ©rait quâ??en le menant, Â« Apple aidera Ã rendre justice Ã tous ceux qui ont Ã©tÃ© des victimes du comportement irresponsable de NSO Group Â».

ParallÃ¨lement Ã Amnesty International, Apple a chargÃ© Citizen Lab de fournir de la documentation sur la faÃ§on dont le logiciel espion Pegasus de NSO Group a Ã©tÃ© utilisÃ© par des gouvernements pour cibler des travailleurs des droits de lâ??homme et des journalistes dans le monde entier.

RÃ©cemment, les deux organisations ont confirmÃ© que Pegasus servait Ã espionner les employÃ©s de plusieurs associations de dÃ©fense des droits de lâ??homme quâ??IsraÃ«l a dÃ©signÃ©es le mois dernier comme Ã©tant Â« terroristes Â» dans le but de salir et de saboter leur travail de documentation

sur ses crimes.

Plus tÃ´t ce mois-ci, un juge fÃ©dÃ©ral amÃ©ricain a refusÃ© une motion de NSO Group pour rejeter une demande de procÃ¨s dÃ©posÃ©e par WhatsApp et sa sociÃ©tÃ© mÃ¨re Facebook â?? maintenant rebaptisÃ©e Meta â?? Ã propos du ciblage en 2019 de 1.400 de ses utilisateurs par le logiciel espion Pegasus.

Parmi les pays oÃ¹ le logiciel espion Pegasus a Ã©tÃ© largement utilisÃ©, il y a le BahreÃ¯n, le Kazakhstan, le Mexique, le Maroc, lâ??Arabie Saoudite et les Ã?mirats Arabes Unis.

Des dizaines de journalistes de nombreux autres pays, dont la Grande Bretagne, la France, lâ??Espagne, la Hongrie et lâ??Inde, ont Ã©tÃ© identifiÃ©s comme des cibles potentielles.

NSO Group dit quâ??il ne vend sa technologie quâ??aux gouvernements.

Â« Nouvelles protections de sÃ©curitÃ© Â» pour les iPhones

Citizen Lab a rÃ©vÃ©lÃ© en octobre quâ??un Ã©minent journaliste du *New York Times*, qui a prÃ©cÃ©demment Ã©crit un reportage sur NSO Group et qui rÃ©dige un livre sur lâ??Arabie Saoudite, avait Ã©tÃ© ciblÃ© Ã plusieurs reprises avec Pegasus.

Le groupe de recherche a dit quâ??il Ã©tait incapable de confirmer qui avait menÃ© ces attaques, mais quâ??il croyait que lâ??opÃ©rateur responsable de lâ??un de ces piratages sur le journaliste du *Times* Â« Ã©tait Ã©galement responsable du piratage du militant saoudien en 2021 Â».

Tout en cherchant Ã empÃªcher dâ??autres violations par NSO Group, Apple rassure Ã©galement ses clients parce quâ??il a bloquÃ© toutes les voies connues par lesquelles Pegasus est venu infecter ses dispositifs.

La sociÃ©tÃ© a dit que son tout dernier systÃ¨me de fonctionnement de lâ??iPhone, IOS 15 Â« contient quantitÃ© de nouvelles protections de sÃ©curitÃ© Â». Apple affirme aussi quâ??il Â« nâ??a observÃ© aucune preuve dâ??attaques Ã distance rÃ©ussies contre les dispositifs qui font marcher IOS 15 et les versions ultÃ©rieures Â».

Apple a redit que les usagers devraient toujours sâ??assurer que leurs appareils sont dotÃ©s des logiciels les plus rÃ©cents.

Â« Les dÃ©marches que nous entreprenons aujourdâ??hui enverront un message clair Â», a dit Ivan Krstic, chef de lâ??ingÃ©nierie de sÃ©curitÃ© dâ??Apple. Â« Dans une sociÃ©tÃ© libre, il est inacceptable dâ??armer de puissants logiciels espions parrainÃ©s par un Ã?tat contre ceux qui cherchent Ã rendre le monde plus vivable. Â»

La sociÃ©tÃ© a dit quâ??elle contribuerait Ã hauteur de 10 millions de dollars ainsi quâ??Ã tous dommages et intÃ©rÃªts consÃ©cutifs au procÃ¨s Â« pour les organisations qui poursuivent la recherche et le plaidoyer sur la cybersurveillance Â».

Les sanctions amÃ©ricaines peuvent mettre lâ??entreprise en faillite

La dÃ©marche dâ??Apple nâ??est que le dernier malheur qui frappe NSO Group.

ParallÃ¨lement Ã une autre sociÃ©tÃ© israÃ©lienne, Candiru, NSO Group a rÃ©cemment Ã©tÃ© mise sur liste noire par le gouvernement amÃ©ricain pour fabrication de logiciel espion utilisÃ© par des gouvernements Ã©trangers Â« pour cibler perfidement des reprÃ©sentants de gouvernements, des journalistes, des hommes dâ??affaires, des militants, des universitaires et des employÃ©s dâ??ambassade Â».

Le logiciel espion de Candiru est soupÃ§onnÃ© dâ??avoir Ã©tÃ© utilisÃ© dans des attaques sur quelque 20 sites internet depuis 2020, dont la publication *Middle East Eye* [Lâ??Å?il du Moyen Orient].

ESET, entreprise de cybersÃ©curitÃ© qui a collectÃ© des renseignements sur les attaques de Candiru, a dit que les cibles avaient Â« des liens avec le Moyen Orient et un intÃ©rÃªt marquÃ© pour le YÃ©men et le conflit environnant Â».

Elle y a aussi inclus des sites internet appartenant au ministÃ¨re iranien des Affaires Ã©trangÃ¨res, au ministÃ¨re syrien de lâ??Ã?lectricitÃ© et un site gÃ©rÃ© par des dissidents saoudiens.

AprÃ¨s sa mise sur liste noire par les AmÃ©ricains, le nouveau PDG de NSO Group a quittÃ© le navire une semaine seulement aprÃ¨s sa nomination.

IsraÃ«l considÃ¨re NSO Group comme Â« un Ã©lÃ©ment essentiel de sa politique Ã©trangÃ¨re et fait pression sur Washington pour retirer la sociÃ©tÃ© de la liste noire Â», a rapportÃ© *The New York Times* plus tÃ´t ce mois-ci.

En attendant, le coÃ»t du dÃ©saccord avec les Ã?tats-Unis â?? qui a dÃ©crit sa mise sur liste noire des entreprises israÃ©liennes comme Â« faisant partie des efforts de lâ??administration Biden-Harris pour mettre les droits de lâ??homme au centre de la politique Ã©trangÃ¨re amÃ©ricaine Â» â?? grimpe.

La cotation de crÃ©dit de la sociÃ©tÃ© Moodyâ??s de cette semaine a dit que NSO Group risquait de perdre 500 millions de dollars de prÃªts parce que les sanctions amÃ©ricaines sur lâ??entreprise rendraient plus difficiles la levÃ©e de fonds et lâ??adhÃ©sion de nouveaux clients.

Menace mondiale provenant dâ??IsraÃ«l

Nonobstant les difficultÃ©s auxquelles font face NSO Group et Candiru, il ne faudrait pas sâ??imaginer que les menaces sur la vie privÃ©e, la libertÃ© dâ??expression et la libertÃ© politique qui Ã©manent de lâ??industrie israÃ©lienne de guerre informatique soutenue par le gouvernement vont diminuer de sitÃ´t.

On dit quâ??IsraÃ«l teste de puissants systÃ¨mes de reconnaissance faciale sur la population palestinienne captive en Cisjordanie occupÃ©e, permettant une surveillance en temps rÃ©el largement Ã©tendue.

IsraÃ«l peut aussi Ã©couter chaque conversation tÃ©lÃ©phonique qui prend place en Cisjordanie et dans la Bande de Gaza, a rapportÃ© *Middle East Eye* au dÃ©but de ce mois, citant un ancien membre de lâ??UnitÃ© 8200, division dâ??espionnage Ã©lectronique de lâ??armÃ©e dâ??IsraÃ«l.

Â« Tout portable ou tÃ©lÃ©phone importÃ© dans Gaza par le passage de Kerem Shalom â?? au sud de Gaza â?? est implantÃ© dâ??une puce israÃ©lienne, et quiconque utilise les deux seuls rÃ©seaux

pour portables installÃ©s dans les territoires occupÃ©s â?? Jawpal et Wataniya â?? est lui aussi surveillÃ© Â», a affirmÃ© la publication, citant le lanceur dâ??alerte anonyme.

Les Palestiniens que cible IsraÃ«l se retrouvent dans deux groupes : dans le premier se trouvent ceux qui ont une activitÃ© politique ou qui reprÃ©sentent ceux quâ??IsraÃ«l considÃ¨re comme une menace pour Â« la sÃ©curitÃ© Â». Le deuxiÃ¨me groupe, ce sont les Palestiniens qui peuvent Ãªtre mis sur liste noire.

Â« Il pourrait sâ??agir de trouver des gays sur qui on peut faire pression pour quâ??ils parlent de leurs proches, ou de trouver un homme qui trompe sa femme Â», a dit lâ??ancien de lâ??UnitÃ© 8200 Ã *Middle East Eye*. Â« Trouver quelquâ??un qui doit de lâ??argent Ã un autre, disons, signifier quâ??on peut le contacter et lui offrir de lâ??argent pour payer sa dette en Ã©change de sa collaboration. Â»

Ce rapport confirme ce quâ??un groupe dâ??anciens de lâ??UnitÃ© 8200 a rÃ©vÃ©lÃ© en 2014 Ã *The Guardian*.

Les informations obtenues grÃ¢ce Ã une surveillance massive des Palestiniens ont Ã©galement servi Ã planifier et exÃ©cuter la violence. Un vÃ©tÃ©ran a dÃ©clarÃ© en 2014 que les membres de lâ??UnitÃ© 8200 utilisaient lâ??expression Â« du sang sur les oreillettes Â», ou traÃ§aient un Â« X Â» sur leur casque aprÃ¨s un assassinat.

De nombreux vÃ©tÃ©rans de lâ??UnitÃ© 8200 accÃ¨dent Ã un emploi lucratif dans des entreprises privÃ©es dâ??espionnage dont Candiru, NSO Group et lâ??entreprise DarkMatter propriÃ©tÃ© des Ã?mirats Arabes Unis.

Une indignation sâ??est Ã©galement manifestÃ©e plus tÃ´t cette annÃ©e parmi les membres du Parti Travailliste de Grande Bretagne aprÃ¨s que lâ??*Electronic Intifada* ait rÃ©vÃ©lÃ© que Keir Starmer avait embauchÃ© un ancien espion de lâ??UnitÃ© 8200 pour travailler dans son bureau quand il a succÃ©dÃ© Ã Jeremy Corbyn Ã la tÃªte du parti.

Traduction : J. Ch. pour lâ??Agence MÃ©dia Palestine

Source : The Electronic Intifada

date crÃ©Ã©e
2021/12/02