19July2021-Pegasus, l’arme informatique qui cible les journalistes, dissidents et politiques

Surveillance

Abonné

Une enquête menée par des dizaines de journalistes révèle l'ampleur de l'espionnage numérique opéré dans 50 000 smartphones du monde entier

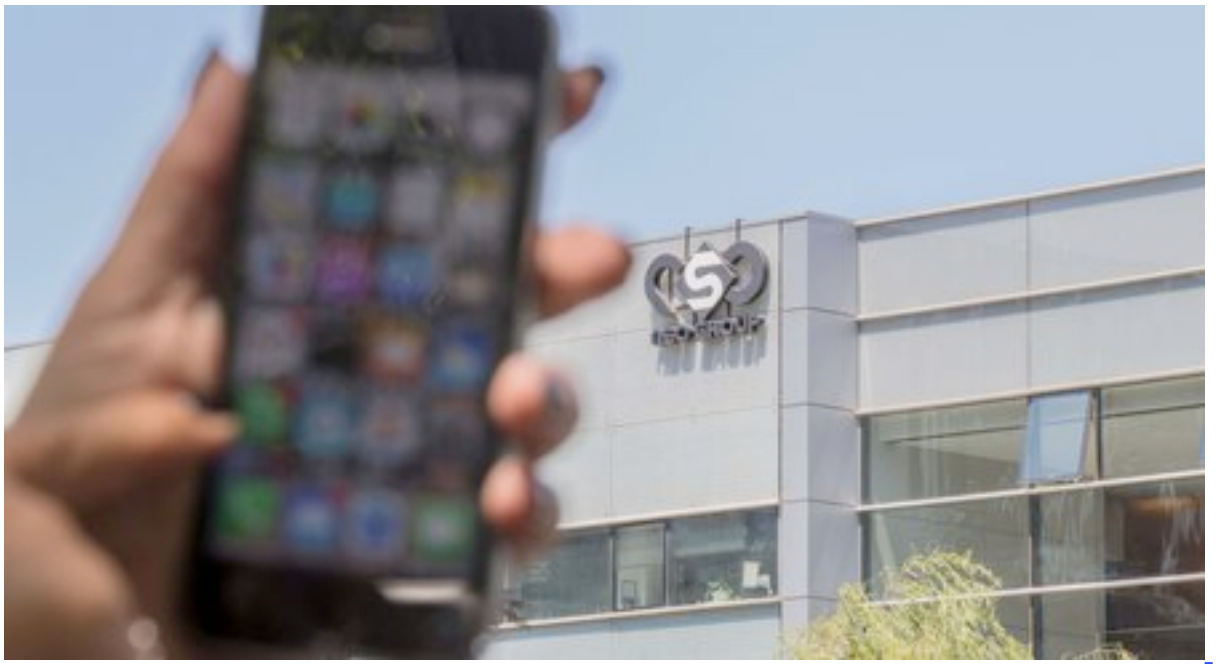

Photo composée devant le siège de NSO, à Herzliya, août 2016. — © JACK GUEZ / AFP

Chams Iaz

Publié lundi 19 juillet 2021 à 15:04
Modifié lundi 19 juillet 2021 à 16:19

Une fuite de 50 000 numéros de téléphone révèle l’étendue d’une surveillance mondiale de journalistes, militants des droits de l’homme, universitaires, syndicalistes, opposants politiques, diplomates, hommes et de femmes politiques et plusieurs chefs d’Etat. Amorcée en 2016, cette vaste opération d’espionnage est orchestrée aussi bien par des services d’Etats que par des entités privées. Les 80 journalistes travaillant pour 17 médias différents* qui ont remonté le fil de cette affaire dévoilent la portée de cette action et dénoncent l’absence de sanctions à l’encontre de son

fournisseur: NSO Group. Le secrétaire général de Reporters sans frontières, Christophe Deloire, signale par voie de communiqué que l'organisation mettra «tout en œuvre pour que l'entreprise NSO soit condamnée pour les forfaits dont elle se rend coupable et les tragédies qu'elle rend possibles.»

Un simple appel en absence

Le logiciel espion développé par l'entreprise israélienne spécialisée dans la sécurité informatique est bien entendu installé dans les smartphones des personnes ciblées à leur insu; mais surtout, il ne nécessite aucune manipulation de leur part. «Aucun lien à cliquer ni document à ouvrir, l'attaque est totalement invisible, note Forbidden Stories, une association à but non-lucratif qui rassemble un consortium de médias locaux et internationaux. «Une fois installé, Pegasus – le nom du logiciel espion en question – donne un accès total au téléphone, y compris aux messages échangés sur des applications chiffrées telles que WhatsApp, Signal ou Telegram, et permet même d'activer à distance le microphone et la caméra de l'appareil.» Celui-ci permet également d'accéder au carnet de contacts et aux données de localisation du téléphone.

Lire aussi: Piratage du mobile de Jeff Bezos: la piste israélienne

Cette technologie intrusive a su bénéficier de l'évolution des usages technologiques. La société a été créée en 2010 par deux amis, Shalev Hulio et Omri Lavie, et un ancien employé du Mossad, Niv Carmi – les initiales de leurs prénoms forment le nom de l'entreprise, NSO. Si à cette période, les logiciels malveillants nécessitaient l'envoi d'un e-mail pour pouvoir être installé sur les équipements. Avec la généralisation des smartphones dès 2014, la méthode s'est adaptée, et l'envoi d'un SMS suffisait. Dans les deux cas, la personne ciblée devait cliquer sur un lien ou procéder à un téléchargement. Désormais, un simple appel, en absence ou non, permet aux auteurs de s'immiscer dans l'appareil, d'aspirer les données, de voir, d'entendre tout ce qu'il se passe dessus et dans ses alentours.

«Dès lors que quelqu'un est en train de lire par-dessus votre épaule, le chiffrement – technologie de cryptage des contenus – importe peu», résume Bruce Schneier, expert en chiffrement et membre du Berkman Klein Center, un centre de recherches de l'université Harvard dédié à l'exploration et la compréhension du cyberespace. Efficace, cette technologie est donc «devenue un outil clé de l'arsenal des gouvernements répressifs et des services de renseignement», affirme le consortium.

Ce dernier estime que parmi les victimes figurent au moins 180 journalistes, ciblés dans vingt pays par au moins dix clients de NSO. Celles et ceux qui apparaissent dans cette liste «ont pour certains reçus des menaces juridiques, d'autres ont été arrêtés ou diffamés, d'autres encore ont fui leur pays et la persécution dont ils étaient victimes, écrit Forbidden Stories. Dans de rares cas, des journalistes ont été assassinés après avoir été sélectionnés comme cibles.»

Aux quatres coins du monde

C'est le cas de Omar Rad, journaliste d'investigation indépendant au Maroc, de Anand Teltumbde, journaliste indien et défenseur des droits humains, de Taoufik Bouachrine, rédacteur en chef

d'*Akhbar al-Youm*, et de Souleimane Raissouni, rédacteur en chef du quotidien indépendant Akhbar al-Youm, qui ont été espionnés et emprisonnés. Mais aussi des journalistes assassinés en 2017 et 2018: le journaliste d'investigation mexicain Cecilio Pineda et le chroniqueur saoudien du *Washington Post* Jamal Khashoggi. Le premier a été pris pour cible par un client de NSO Group basé au Mexique. La fiancée du second, son fils, un ami proche et l'enquêteur en chef turc chargé de son crime ont été espionnés par un client de la compagnie basé aux Emirats arabes unis.

Car même si une première étude conduite en 2018 par les experts de l'institut de recherche canadien Citizen Lab avait déjà découvert que Pegasus était actif dans 45 pays, l'enquête journalistique sur ce logiciel démontre que les clients de NSO Group sont aussi bien des régimes autocratiques que des Etats démocratiques. Ainsi, des dizaines de milliers de numéros ont été traquées par des clients installés en Arabie Saoudite, au Maroc et au Bahreïn. Les autres, en Inde, au Mexique, en Hongrie, en Azerbaïdjan, en France, au Togo, ou encore au Rwanda. NSO Groupe n'a pu «ni confirmer ni nier» cette liste, faisant valoir des «considérations contractuelles et de sécurité nationale».

Dans son rapport de transparence publié en juin 2021, la société israélienne assure que ses outils sont exclusivement utilisés pour cibler de dangereux criminels et des terroristes. Elle ajoute, sans préciser lesquels, s'être séparée de cinq clients au cours des dernières années en raison de problèmes de droits humains. Danna Ingleton, la directrice adjointe d'Amnesty Tech a déclaré à la *Sueddeutsche* Zeitung que «l'entreprise ne peut plus se cacher derrière ce mensonge et se laver les mains de son innocence en ce qui concerne les violations des droits humains causées par sa technologie invasive.»

Interrogée en août 2018 par CBS News, Tami Shachar, la coprésidente de NSO Group, répondait que «pour se protéger contre les abus, la NSO a mis en place trois niveaux de contrôle des clients potentiels: un premier par le ministère israélien de la Défense, un deuxième par son propre comité d'éthique et un troisième en leur faisant signer une clause stipulant que le système ne sera utilisé que pour lutter contre le terrorisme et la criminalité.»

Une corrélation selon la date d'infection

Pourtant, la fuite des 50 000 numéros ciblés par ses clients indique qu'entre 2017 et 2018, plus de 2000 numéros indiens et pakistanais ont été enregistrés, «dont ceux de journalistes travaillant pour *The Hindu*, *Hindustan Times*, l'*Indian Express*, *India Today*, *Tribune*, et le site d'investigation *Tehelka*», détaille Forbidden Stories. Mais aussi Jaspal Singh Heran, rédacteur en chef d'un média basé dans le Pendjab et Siddarth Varadarajan, journaliste d'investigation et fondateur du site *The Wire*. Le téléphone de ce dernier a été hacké en 2018. Celui du cofondateur de *The Wire*, MK Venu, a été piraté le mois dernier. Des personnes liées à ce média ont également été ciblées: l'éditorialiste Prem Shankar Jha et les journalistes Robini Singh et Devirupa Mitra.

D'après *Le Monde*, média membre du consortium, en ciblant des journalistes, diplomates étrangers, militants, humanitaires ou politiciens de tous bords, le client indien de NSO Group semble être au service de Narendra Modi. Le journal français souligne dans son article que l'utilisation du logiciel Pegasus a commencé juste après la visite du Premier ministre indien en Israël, en juillet 2017.

Les dates d'infection des smartphones ont parfois permis aux journalistes de comprendre les motivations des intrus. Paranjoy Guha Thakurta, un journaliste d'investigation indien a par exemple été espionné dès 2018, alors qu'il enquêtait sur les finances de Drirubhai Ambani, un Indien aujourd'hui décédé, l'un des hommes les plus riches du pays. Szabolcs Panyi, un journaliste

d'investigation hongrois du site Direkt36 a été surveillé pendant sept mois en 2019, quand il s'intéressait à deux sujets sensibles et qu'il avait transmis des demandes officielles de commentaires. Edwy Plenel, le directeur et cofondateur du site d'investigation indépendant Mediapart, est lui aussi ciblé depuis l'été 2019, période durant laquelle il avait rencontré à Essaouira Hicham Mansouri, journaliste d'investigation indépendant et cofondateur de l'Association Marocaines des Journalistes d'Investigation.

Le numéro de ce dernier est également surveillé. Tout comme celui de Lénaïg Bredoux, journaliste à Mediapart, d'Ali Amar, fondateur du magazine d'investigation marocain LeDesk, Ben Hubbard, journaliste du *New York Times*, Roula Khalaf, rédactrice en chef du *Financial Times*, Khadija Ismayilova, journaliste indépendante azerbaïdjanaise installée en Turquie, ou Carmen Aristegui, journaliste d'investigation mexicaine, mais aussi ses collègues Sebastian Barragan et Rafael Cabrera, son fils Emilio Aristegui, sa sœur Teresa Aristegui, sa productrice à CNN Karina Maciel, et son ancienne assistante Sandra Nogales. La liste des personnes concernées présentée dans cette enquête n'est pas exhaustive, car les révélations publiées ces dernières heures ne constituent que son premier volet.

Lire également: Comment tenter de se protéger contre le logiciel espion Pegasus

Les téléphones ciblés encore en usage ou conservés par leurs propriétaires ont été examinés par le Security Lab d'Amnesty International, puis par le Citizen Lab. «L'analyse technique de ces téléphones a pu confirmer une infection ou tentative d'infection avec le logiciel espion Pegasus dans 85% des cas, soit 37 au total, détaille Forbidden Stories. Ce taux est remarquablement élevé étant donné que le logiciel espion, à la pointe de la technologie, est censé être indétectable.» A ce stade, l'enquête souligne que pour s'introduire dans les smartphones, NSO Group exploite une faille de sécurité des iPhones. Cette brèche n'est toujours pas réparée et existe également sur les derniers modèles.

Liste des membres de ce consortium:

The Guardian, Le Monde, The Washington Post, Süddeutsche Zeitung, Die Zeit, Aristegui Noticias, Radio France, Proceso, OCCRP, Knack, Le Soir, Haaretz/TheMarker, The Wire, Daraj, Direkt36, PBS Frontline.