MARDI 20 JUILLET 2021
77e ANNÉE – N° 23803
3,00 € – FRANCE MÉTROPOLITAINE
WWW.LEMONDE.FR –
FONDATEUR : HUBERT BEUVE-MÉRY
DIRECTEUR : JÉRÔME FENOGLIO

Le Monde

PROJET PEGASUS

RÉVÉLATIONS SUR UN SYSTÈME MONDIAL D'ESPIONNAGE DE TÉLÉPHONES

Hommes politiques, avocats, militants et journalistes sont les premières victimes

▸ Depuis 2016, des dizaines de milliers de téléphones ont été sélectionnés comme cibles d'un logiciel d'espionnage baptisé « Pegasus », commercialisé par la société israélienne NSO

▸ Six mois d'une enquête internationale réunissant dix-sept médias, dont « Le Monde », montrent que cet outil, officiellement destiné à lutter contre le terrorisme, est massivement utilisé pour surveiller les sociétés civiles

▸ En France, un millier de numéros ont été visés, notamment pour le compte du Maroc

PAGES 2 À 6

ILLUSTRATION « LE MONDE », D'APRÈS JACK GUEZ/AFP

ÉDITORIAL

QUAND LA DÉRIVE DEVIENT LA NORME

par JÉRÔME FENOGLIO

DEPUIS des années, des réponses invariablement lénifiantes sont opposées aux nombreuses inquiétudes sur les dérives potentiellement liberticides rendues possibles par les outils créés par l'industrie de la surveillance numérique. Les entreprises de ce secteur, comme les États qui font appel à leurs services, assurent que les risques sont infimes, les usages encadrés, les engagements respectés. Depuis des années, les doutes sont balayés au nom de l'intérêt supérieur des sécurités nationales et de la lutte contre le terrorisme ou le crime organisé.

Cette négation de l'évidence sera désormais beaucoup plus compliquée. Les révélations publiées au long de cette semaine par *Le Monde* et seize rédactions associées au sein du « Projet Pegasus », coordonnées par l'organisation Forbidden Stories, en partenariat avec Amnesty International, prouvent, de manière incontestable, qu'en matière de cybersurveillance l'abus est la règle et non l'exception.

LIRE LA SUITE PAGE 28

Inondations

En Allemagne, après le déluge et les morts, le temps des questions

PAGES 10-11

Salvador

L'insolente popularité de l'autoritaire président Bukele

PAGE 7

Culture

L'énergie poétique d'Emma Dante réveille le Festival d'Avignon

PAGE 18

L'été des séries

Elon Musk
Itinéraire d'un ambitieux qui nourrit les rêves de l'Amérique
PAGES 22-23

Vocations en séries
Du « Bureau des légendes » à la DGSE
PAGE 24

Un train d'avance
« Le train est un objet jubilatoire », confie le dessinateur ferroviphile François Schuiten
PAGE 26

A Hawthorne, en Californie, le 14 mars 2019. AP

Politique

Le projet de loi sanitaire examiné dans un contexte tendu

Le gouvernement vise une adoption en fin de semaine. Samedi, 110 000 opposants au passe sanitaire ont manifesté
PAGE 12

Angleterre

Boris Johnson lève les restrictions malgré le Delta

La stratégie du gouvernement fait débat, alors que le pays enregistre chaque jour plus de 50 000 nouveaux cas de Covid-19
PAGE 9

EspaceTopper
Maison familiale à Paris depuis 1926
95 ans
Offres
ANNIVERSAIRE
Système d'ouverture rapide. Haute résilience 35kg/m³. L 177 x P 100 x H 89. Nombreux coloris, existe en 160. Prix livré-installé, coussins déco en option.
Canapé-lit 140 extra moelleux
Matelas 15 cm Dunlopillo
1590€
Présenté en tissu Miami 100% polyester
CANAPÉS, LITERIE MOBILIER : 3 000 M² D'ENVIES ! Toutes nos adresses sur www.topper.fr
Canapés-lits Paris 15 • 7j/7
63 rue de la Convention, 01 45 77 80 40
M° Boucicaut, parking gratuit
Canapés-lits Paris 12 • 7j/7
54 cours de Vincennes, 01 40 21 87 53
M° Porte de Vincennes ou Nation

Algérie 220 DA, **Allemagne** 3,80 €, **Andorre** 3,80 €, **Autriche** 3,80 €, **Belgique** 3,30 €, **Canada** 5,80 $ Can, **Chypre** 3,20 €, **Danemark** 36 KRD, **Espagne** 3,60 €, **Gabon** 2 400 F CFA, **Grande-Bretagne** 3,20 £, **Grèce** 3,50 €, **Guadeloupe-Martinique** 3,30 €, **Hongrie** 1 460 HUF, **Italie** 3,50 €, **Luxembourg** 3,30 €, **Malte** 3,20 €, **Maroc** 23 DH, **Pays-Bas** 4,00 €, **Portugal cont.** 3,50 €, **La Réunion** 3,30 €, **Sénégal** 2 400 F CFA, **Suisse** 4,50 CHF, **TOM Avion** 500 XPF, **Tunisie** 4,50 DT, **Afrique CFA autres** 2 400 F CFA

Le Monde
MARDI 20 JUILLET 2021

ILLUSTRATION « LE MONDE », D'APRÈS CORINNA KERN/NYT-REDUX-REA

Pegasus, la surveillance en toute impunité

Un logiciel de la société israélienne NSO a permis à des Etats de cibler des dizaines de milliers de smartphones

C'est un annuaire ahurissant, dans lequel on trouve un chef d'Etat et deux chefs de gouvernement européens ; des hommes et des femmes aux plus hauts échelons du pouvoir d'une ex-République soviétique ; des dizaines de députés de l'opposition d'un pays africain ; des princes et des princesses, des chefs d'entreprise, quelques milliardaires, des ambassadeurs, des généraux. Et puis, aussi et surtout, des centaines de journalistes, d'avocats, de militants des droits de l'homme.

Le Monde, associé au sein d'un consortium à seize autres rédactions, a eu accès à environ 50 000 numéros de téléphone – partagés par l'organisation Forbidden Stories et Amnesty International – de cibles potentielles du logiciel espion Pegasus, conçu par la société israélienne NSO Group, pour le compte d'une dizaine de gouvernements. Il s'avère que nombre de ces cibles au sein de la société civile ont été effectivement infectées par Pegasus. *Le Monde* et le consortium coordonné par Forbidden Stories ont pu confirmer l'authenticité des données en les croisant avec plusieurs autres sources et en identifiant des dizaines de nouvelles victimes du logiciel par des analyses techniques extrêmement poussées sur leurs téléphones mobiles, grâce aux experts du Security Lab d'Amnesty International.

Ces listes de « cibles » sont d'un intérêt exceptionnel : l'usage de Pegasus que font les Etats clients de NSO, en dehors de tout cadre légal, est un secret bien gardé. Depuis sa création, en 2011, l'entreprise israélienne vend son logiciel comme un outil décisif, destiné uniquement à la lutte contre le terrorisme et le crime organisé – et multiplie les discours assurant que tout est mis en œuvre pour garantir cet usage « légitime ». L'analyse des données consultées par *Le Monde* et ses partenaires montre que, pour une grande partie des clients de NSO, terrorisme et grand banditisme ne constituent qu'une infime partie des utilisations.

En Azerbaïdjan, au Maroc ou au Rwanda, ce sont avant tout des journalistes, des opposants, des avocats, des défenseurs des droits de l'homme qui sont les principales cibles de ce logiciel espion sophistiqué. NSO répète depuis des années que les cas de surveillance politique sont des incidents isolés. Les informations que *Le Monde* et ses partenaires publient, dans une série de révélations programmées tout au long de la semaine, prouvent de manière incontestable que ces abus sont la norme et non l'exception.

Outil de « soft power »

Ces violations des droits de l'homme répétées sont commises par des Etats pour lesquels la vente de Pegasus a été systématiquement validée par le ministère de la défense israélien. Israël protège et choie NSO, un outil de son « soft power », dont la fourniture à des gouvernements a pu contribuer à la restauration de relations diplomatiques. Les activités de NSO éclairent, en partie, les rapprochements récents de l'Etat hébreu avec l'Arabie saoudite, la Hongrie ou le Maroc.

Ni NSO ni le gouvernement israélien ne peuvent ignorer qu'une importante partie de leurs clients achètent Pegasus spécifiquement pour se livrer à une surveillance de leurs oppositions politiques et de leur population, sans oublier l'espionnage industriel de leurs partenaires commerciaux et le renseignement sur les gouvernements voisins. La législation internationale n'encadre qu'à la marge les ventes de ces armes informatiques, que leurs acheteurs utilisent quotidiennement contre des civils, et même contre des populations protégées par la convention de Genève, comme les médecins.

LES ACTIVITÉS DE NSO ÉCLAIRENT, EN PARTIE, LES RAPPROCHEMENTS RÉCENTS D'ISRAËL AVEC L'ARABIE SAOUDITE, LA HONGRIE OU LE MAROC

« NSO Group nie fermement les fausses accusations portées dans votre enquête. Ces accusations sont pour beaucoup des théories non corroborées, qui jettent de sérieux doutes sur la crédibilité de vos sources, ainsi que sur le cœur de votre enquête », a répondu l'entreprise israélienne, contactée par le « Projet Pegasus ». *« Vos sources vous ont fourni des informations ne s'appuyant sur aucune base factuelle »*, ajoute la société, qui affirme ne pas connaître en temps réel l'usage fait par ses clients de Pegasus, ni le contrôler. *« NSO Group continuera d'enquêter sur les accusations crédibles d'utilisation abusive* [de son logiciel] *et agira en fonction des résultats de ces enquêtes. Cela pourra consister en l'interruption de l'accès de certains clients au système en cas d'abus confirmés. Il l'a fait par le passé et n'hésitera pas à le réitérer »*, a précisé l'entreprise.

L'ampleur et la gravité de ces violations des droits de l'homme tient aussi à la nature de Pegasus, qui n'est pas un simple outil « d'écoute téléphonique ». Réputé particulièrement efficace et puissant, le logiciel espion peut aspirer l'ensemble des données contenues dans un téléphone, depuis les photographies ou les carnets d'adresses jusqu'aux messages échangés sur des applications, pourtant sécurisées, comme Signal ou WhatsApp.

Discrétion et facilité d'usage

Invisible pour l'utilisateur du téléphone, ce logiciel peut être installé à distance, sans que la cible ait même besoin de cliquer sur un lien malveillant, et en toute discrétion, en s'appuyant sur des failles de sécurité dans les logiciels d'Apple et de Google, que ces géants ne corrigent pas toujours assez vite. Le logiciel de NSO alimente aussi un lucratif et obscur marché des failles de sécurité, incitant des centaines de pirates chevronnés à rechercher en permanence de nouvelles vulnérabilités que NSO et une poignée d'autres acteurs achètent au prix fort.

Cette discrétion et cette facilité d'usage ont également fait de Pegasus un outil d'espionnage de choix entre Etats. Plus que d'autres pays, la France en a fait les frais ; plusieurs milliers de numéros téléphoniques en « +33 », l'indicatif français, ont été ciblés par Pegasus, la majorité pour le compte d'un pays « allié » de la France, le Maroc – sollicité, Rabat *« rejette catégoriquement les allégations »* faisant état d'une *« quelconque relation entre le Maroc et la compagnie israélienne* [NSO] ». Des diplomates, des hauts fonctionnaires, des élus : le logiciel de NSO a permis au Maroc, pour un tarif modique, de cibler, en quelques clics, des pans entiers de notre appareil d'Etat. Les plus cyniques y verront la marche habituelle des rapports entre pays. Mais les enquêtes du *Monde* et de ses partenaires montrent que ce vaste système de surveillance dépasse de très loin le cadre du jeu « normal » de l'espionnage.

En France comme dans les pays qui ont acheté l'accès à ce logiciel espion, c'est aussi et surtout la société civile qui est visée : des athlètes, des prêtres et des imams, des journalistes, des youtubeurs, des avocats. Et aussi des hommes et des femmes dont le seul tort est d'être proches, par liens d'amitié ou familial, de personnes critiques du gouvernement. Les témoignages recueillis par les journalistes du « Projet Pegasus » soulignent les conséquences dramatiques de cette surveillance, dans la vie personnelle des cibles comme dans la manière dont elle conduit à l'autocensure de voix dissidentes, même les plus modérées.

« Projet Pegasus » n'est pas l'histoire d'un scandale de surveillance de masse, comme l'ont été les révélations d'Edward Snowden sur les opérations menées par la NSA américaine, en 2013. Les victimes de Pegasus ont été ciblées, individuellement, par des gouvernements et des services de renseignement. Mais ces deux scandales ont un point commun : ils montrent à quel point les espions qui utilisent les outils les plus perfectionnés pour surveiller et contrôler les moindres détails de la vie de leurs cibles n'ont jamais de comptes à rendre. ■

DAMIEN LELOUP
ET MARTIN UNTERSINGER

CE QU'IL FAUT SAVOIR

Pegasus. Le logiciel espion Pegasus est capable d'aspirer tout le contenu d'un téléphone : messages, e-mails, photos, carnet d'adresses… Les dernières versions, qui fonctionnent sur Android comme sur iPhone, peuvent être installées sans action de l'utilisateur, et sans que rien n'indique que le téléphone est piraté. Le logiciel est conçu par la société israélienne NSO Group, qui le vend exclusivement aux Etats.

Le « Projet Pegasus ». *Le Monde* et seize autres médias, réunis au sein d'un consortium coordonné par l'équipe de Forbidden Stories, ont pu consulter, avec l'appui d'Amnesty International, une liste de plus de 50 000 numéros de téléphone sélectionnés comme cibles potentielles de Pegasus depuis 2016 pour le compte d'une dizaine d'Etats. Le projet a réuni les rédactions d'*Aristegui Noticias, Daraj, Die Zeit, Direkt 36, Knack, Forbidden Stories, Haaretz, Le Monde, OCCRP, Proceso, PBS Frontline, Radio France, Le Soir, Süddeutsche Zeitung, The Guardian, The Washington Post* et *The Wire*.

Toute la semaine, *Le Monde* publiera des révélations.

« Jamal m'avait dit que cela pouvait arriver »

Les téléphones de proches de l'opposant au régime saoudien assassiné ont été infectés par le logiciel espion

L'entourage de Jamal Khashoggi, l'éditorialiste saoudien du *Washington Post* assassiné le 2 octobre 2018, était sous surveillance. Plusieurs mois d'une enquête menée par Forbidden Stories et seize médias, dont le *Washington Post* et *Le Monde*, permettent d'affirmer que deux femmes intimes de la victime ont été visées par Pegasus. Une analyse technique démontre même la présence de ce logiciel espion dans le téléphone d'une d'elles quelques jours après l'assassinat.

NSO Group, l'entreprise israélienne qui commercialise ce logiciel espion ultrasophistiqué, a toujours affirmé que son outil n'avait jamais été utilisé pour surveiller M. Khashoggi ou sa famille. Pourtant, le téléphone d'Hanan El-Atr, une hôtesse de l'air égyptienne dont M. Khashoggi était tombé amoureux, a fait l'objet de tentatives d'infections par Pegasus. Quatre SMS contenant des liens qui, en cas de clic, auraient permis au logiciel espion de pénétrer le téléphone, lui ont été envoyés en novembre 2017 et en avril 2018, plusieurs mois avant l'assassinat de M. Khashoggi. En raison de limitations techniques propres à Android, le logiciel qui équipe son téléphone, il n'a pas été possible de déterminer si l'appareil avait été réellement infecté.

A la période où elle a été visée par Pegasus, Mme El-Atr se souvient avoir rencontré Jamal Khashoggi à trois reprises et avoir échangé de nombreux messages et appels avec lui. Il lui avait appris à jongler entre les différentes applications de discussion, pensant ainsi déjouer la surveillance. *« Jamal m'avait dit que cela pouvait arriver,* se souvient Mme El-Atr, depuis les Etats-Unis, après avoir appris le piratage. *Cela me laisse penser que* [les espions] *savaient tout ce qui arrivait à Jamal à travers moi »*, poursuit-elle, racontant qu'à l'époque, elle posait souvent son portable sur la table basse de son salon. Pegasus peut non seulement aspirer le contenu d'un téléphone, mais aussi le transformer, de manière invisible, en micro.

Hatice Cengiz, la fiancée turque de Jamal Khashoggi, a elle aussi été victime de Pegasus, quelques jours après l'assassinat du journaliste. C'est elle qui l'avait accompagné devant le consulat saoudien d'Istanbul le jour de sa mort, et son téléphone a été infecté à plusieurs reprises la semaine suivante, selon une analyse technique menée par Amnesty International. La première infection a eu lieu quatre jours après le meurtre. *« Je suis un peu sous le choc. Je m'y attendais, mais je suis en colère. Je veux être une personne normale, comme tout le monde. Tout ça me terrifie »*, a réagi la jeune femme en apprenant qu'elle avait été espionnée. Le téléphone de Jamal Khashoggi, lui, a été donné par Mme Cengiz aux autorités turques après la mort du journaliste. Ces dernières, qui détiennent toujours l'appareil, refusent de dire s'il a été piraté, en raison de l'enquête judiciaire en cours.

Sollicité par les médias du « Projet Pegasus » et interrogé sur les traces retrouvées sur les téléphones des victimes, NSO Group a à nouveau nié que sa technologie ait été utilisée contre M. Khashoggi ou ses proches. *« Comme nous l'avons déjà expliqué, notre technologie n'a été associée en aucune manière avec le meurtre abominable de Jamal Khashoggi,* a répondu l'entreprise. *Notre technologie n'a permis ni l'écoute, ni le suivi, ni le pistage, ni la collecte d'information. Nous avons déjà enquêté sur ces affirmations sans fondement immédiatement après ce meurtre odieux. »*

Reste que le téléphone d'un autre proche de M. Khashoggi, Wadah Khanfar, ex-journaliste de la télévision qatarie Al-Jazira, a aussi été piraté, selon une analyse technique réalisée par le Security Lab d'Amnesty International. *« Je pense que mon téléphone, ou celui d'Hatice, a pu être piraté à cause de certaines conversations que nous avons eues au moment de la disparition de Jamal »*, a-t-il expliqué aux membres du « Projet Pegasus ».

Des soutiens du journaliste Jamal Khashoggi manifestent devant le consulat d'Arabie saoudite à Istanbul, le 2 octobre 2020, deux ans après son assassinat.
OZAN KOSE/AFP

Des enquêteurs turcs surveillés

Les numéros d'autres proches du chroniqueur assassiné figurent parmi la liste des 50 000 numéros sélectionnés par des clients de Pegasus en vue d'une potentielle infection. Il s'agit de ceux du journaliste turc Turan Kachlakji et de celui d'un militant des droits de l'homme exilé à Londres, qui, craignant pour sa sécurité, a souhaité conserver l'anonymat.

Deux responsables turcs impliqués de près dans l'enquête sur le meurtre de l'éditorialiste figurent également dans cette liste : le procureur Irfan Fidan et un membre influent du parti conservateur au pouvoir, Yasin Aktay. Aucun d'entre eux n'a accepté de faire analyser son téléphone afin de vérifier s'ils avaient bien été infectés. Mais M. Aktay affirme que, peu après l'assassinat, des responsables des renseignements turcs l'ont contacté pour le prévenir que son iPhone avait été piraté et qu'il avait été surveillé, sans dire par qui, mais en lui conseillant de s'en débarrasser. Les renseignements turcs n'ont pas souhaité répondre à nos questions.

> **« JE PENSE QUE MON TÉLÉPHONE, OU CELUI D'HATICE [CENGIZ, SA FIANCÉE], A PU ÊTRE PIRATÉ À CAUSE DE CONVERSATIONS QUE NOUS AVONS EUES AU MOMENT DE LA DISPARITION DE JAMAL »**
> **WADAH KHANFAR**
> ancien journaliste d'Al-Jazira

Selon M. Aktay, les services de renseignement lui ont fourni plusieurs protections, dont un garde du corps et une voiture équipée de sirènes de police. Une protection qui aurait également été accordée à Mme Cengiz, à la suite de menaces de mort reçues sur Internet. Après la mort de M. Khashoggi, en effet, Aktay est devenu un critique virulent de la monarchie saoudienne et continue aujourd'hui à écrire sur l'assassinat de l'éditorialiste et à partager ses articles. Une position qui lui a valu, selon lui, la surveillance du royaume. Il estime d'ailleurs qu'*« ils veulent tuer jusqu'au fantôme de Jamal Khashoggi »*.

Dans un rapport, la direction du renseignement des Etats-Unis a estimé que le prince héritier d'Arabie saoudite, Mohammed Ben Salman, avait bien *« validé »* l'opération ayant conduit à l'assassinat du journaliste à Istanbul. Pour Agnès Callamard, secrétaire générale d'Amnesty International et ex-rapporteuse pour les Nations unies qui a enquêté sur la mort de M. Khashoggi, l'utilisation de Pegasus contre des enquêteurs turcs et des proches du journaliste assassiné *« indique une tentative d'aller au-devant des révélations potentielles »*. Selon elle, le gouvernement saoudien a *« vu la Turquie comme l'endroit primordial à contrôler »*. Question diplomatie, une guerre froide opposait en effet la Turquie, le Qatar et l'Iran à l'Arabie saoudite, à l'Egypte, aux Emirats arabes unis et à Barheïn. Dans ce contexte, le président turc, Recep Tayyip Erdogan, qui emprisonne pourtant des journalistes et blogueurs critiques de son gouvernement, s'était lié d'amitié avec M. Khashoggi.

Des vies brisées

Le sort d'Hatice Cengiz et d'Hanan El-Atr illustre les conséquences de l'espionnage sur les proches des personnes ciblées. Toutes les deux menaient en effet une vie heureuse et libre avant de nouer une relation amoureuse avec le journaliste. Aujourd'hui, elles vivent recluses, abandonnées même de certains de leurs amis qui craignent pour leur sécurité si la moindre connexion avec elles était découverte par les autorités, qu'il s'agisse d'un lien téléphonique, sur les réseaux sociaux, ou même limité à des SMS.

Mme El-Atr perd sa quiétude dès mars 2018, quand elle entame une relation avec l'éditorialiste du *Washington Post*. En avril, les autorités émiraties lui confisquent son téléphone, la détiennent et l'interrogent à plusieurs reprises. Deux fois, elle est assignée à résidence durant plusieurs semaines. Selon elle, les autorités soupçonnent alors M. Khashoggi de monter un réseau secret pour faire tomber des autocrates au Moyen-Orient, alors qu'il cherchait simplement à construire une organisation médiatique indépendante. Aujourd'hui, Hanan El-Atr vit cachée près de Washington et a demandé l'asile politique. C'est pour ses proches et sa famille qu'elle craint le plus, d'autant que certains d'entre eux ont été interrogés par les autorités. *« Je veux juste qu'ils me laissent en paix. Laissez-moi en paix, je vous en prie »*, demande-t-elle.

Avant que Jamal Khashoggi n'entre dans sa vie, Hatice Cengiz était chercheuse et menait des enquêtes de terrain au Moyen-Orient. *« Avant de le rencontrer, je vivais une vie très riche. Je travaillais beaucoup, j'avais des choses à faire tous les jours »*, explique-t-elle. Aujourd'hui, elle ne peut même pas reprendre ses études en tant qu'experte du golfe Persique. *« Je ne peux voyager dans aucun pays arabe. Vous imaginez ? »… « Je paye le prix, mais de quoi ? »*, demande-t-elle. *« Les meurtriers, eux, n'ont rien eu à payer. »* ■

ARTHUR BOUVART (FORBIDDEN STORIES), SOUAD MEKHENNET ET DANA PRIEST (« THE WASHINGTON POST »)

Comment les données du « Projet Pegasus » ont été analysées

LES RÉVÉLATIONS sur l'utilisation du logiciel espion de NSO Group, que publient cette semaine *Le Monde* et seize rédactions coordonnées par l'organisation Forbidden Stories, avec l'appui technique d'Amnesty International, se basent sur une liste de plus de 50 000 numéros de téléphone, présélectionnés par certains clients de NSO Group pour une éventuelle mise sous surveillance.

L'authenticité de cette liste a été corroborée par plusieurs sources, notamment par croisement avec les numéros de victimes déjà identifiées, publiquement ou non, de Pegasus. Surtout, les experts en sécurité informatique du Security Lab d'Amnesty International ont analysé des téléphones dont les numéros figurent dans cette liste, qui n'avaient jamais été identifiés comme cibles de Pegasus, et y ont détecté dans une majorité de cas des traces d'attaque ou d'infection.

Au total, 67 téléphones dont le numéro était dans la liste ont été analysés, et 37 d'entre eux avaient des traces de Pegasus. L'enquête technique a également révélé que, à 84 reprises, la présélection d'un numéro dans la liste a été immédiatement suivie par l'apparition de traces techniques de Pegasus sur les téléphones concernés (certains téléphones analysés ont été ciblés à plusieurs reprises). La méthodologie du Security Lab d'Amnesty International, explicitée dans un rapport technique public et détaillé, a été validée de manière indépendante par les chercheurs du Citizen Lab de l'université de Toronto, experts dans la détection des logiciels espions, et spécialisés dans l'analyse de Pegasus.

Examen technique des téléphones

D'après l'enquête menée pendant six mois par les rédactions du « Projet Pegasus », la présence d'un numéro dans cette liste ne signifie pas automatiquement que le téléphone ait été infecté. Cette liste rassemble des numéros présélectionnés pour une éventuelle infection par des clients de NSO. Certains d'entre eux semblent n'avoir jamais été visés ; d'autres l'ont été sans que l'infection réussisse ; d'autres, enfin, ont été infectés par Pegasus. Nos articles précisent lorsqu'un examen du téléphone a permis de confirmer une infection.

Les données analysées par les rédactions du « Projet Pegasus » ne sont pas exhaustives. Elles semblent ne couvrir qu'une dizaine de pays clients de NSO Group, alors que l'entreprise affirme en compter une quarantaine. Les données ont permis de confirmer l'identité de certains de ces clients, telle la Hongrie.

De son côté, NSO nie que la liste de 50 000 numéros analysée provienne de Pegasus. L'entreprise israélienne, dans une réponse au « Projet Pegasus », suggère que cette liste pourrait provenir d'un service de recherche HLR – un outil d'analyse des informations liées à un téléphone utilisant un réseau, qui n'est pas lié à NSO. Néanmoins, selon une source ayant une connaissance directe des activités de NSO, un tel outil est directement intégré aux services vendus par l'entreprise avec son logiciel espion Pegasus.

Une recherche HLR peut en effet révéler des informations cruciales sur un téléphone, comme sa localisation, le fait qu'il soit actif ou non, etc. *« La raison la plus importante pour laquelle il faut* [à NSO] *un service de recherche HLR est que cela permet de savoir si un téléphone est allumé »*, explique au « Projet Pegasus » l'expert en télécommunications Karsten Nohl, de Security Research Labs, en Allemagne. ■

Le Monde
MARDI 20 JUILLET 2021

De Rabat à Paris, le Maroc ne lâche pas les journalistes

Un service de sécurité a ciblé les rédactions critiques du pouvoir marocain, mais aussi le patron de « Mediapart », Edwy Plenel, ou une journaliste du « Monde »

Les téléphonse du Marocain Omar Radi, de l'Azerbaïdjanaise Khadija Ismayilova, du Français Edwy Plenel et de l'Indien Siddharth Varadarajan, tous journalistes d'investigation, ont été infectés par Pegasus. ABDELJALIL BOUNHAR/AP, AZIZ KARIMOV/PACIFIC PRESS/ZUMA/REA, JOËL SAGET/AFP, REBECCA CONWAY/ NYT/REDUX/REA

Depuis la révélation par Amnesty International, en 2020, de l'infection du téléphone du journaliste marocain d'investigation Omar Radi par le logiciel espion Pegasus, les journalistes marocains indépendants se doutaient bien qu'ils pouvaient être ciblés, eux aussi, par le puissant programme de surveillance commercialisé par l'entreprise israélienne NSO Group. Les listes de numéros de téléphone sélectionnés comme des cibles potentielles dans l'outil de NSO par plusieurs de ses clients, que l'organisation Forbidden Stories et Amnesty International ont partagées avec dix-sept rédactions, dont *Le Monde*, confirment qu'un service de sécurité marocain a utilisé Pegasus pour viser, de manière systématique, des journalistes critiques du pouvoir, et des dirigeants des grandes rédactions du pays.

Le numéro de Taoufik Bouachrine, directeur du journal *Akhbar Al-Yaoum*, qui purge actuellement une peine de quinze ans de prison pour viol, au terme d'un procès dénoncé comme entièrement politique par ses soutiens, a ainsi été entré comme cible potentielle dans le logiciel espion de NSO, ainsi que celui de sa femme. Les numéros d'au moins cinq des plaignantes dont les témoignages ont été utilisés contre lui durant son procès figurent également parmi les cibles potentielles de Pegasus. Une partie des quinze témoins à charge s'étaient rétractés avant le procès, affirmant avoir été contraintes par la police de produire de faux témoignages. Les numéros d'au moins deux plaignantes se trouvant dans ce cas ont été sélectionnés dans l'outil.

Au-delà des cas précis d'Omar Radi et de Taoufik Bouachrine, ce sont tous les patrons de médias indépendants, ou presque, qui semblent avoir intéressé les services de renseignement marocains. Parmi leurs cibles potentielles, on trouve ainsi les fondateurs du *Desk*, Ali Amar, ou celui du site *Badil*, Hamid El-Mahdaoui, condamné à trois ans de prison en 2018 pour sa « participation » au mouvement social du Rif, sévèrement réprimé. Les espions marocains ont également sélectionné pour surveillance potentielle un téléphone utilisé par Omar Brouksy, ancien correspondant de l'AFP et auteur de deux livres critiques sur Mohammed VI et les relations franco-marocaines, tous deux interdits de vente au Maroc. Notifié qu'il avait été une cible potentielle par *Le Monde*, le journaliste espagnol Ignacio Cembrero (*Orient XXI*) explique qu'il n'est *« malheureusement pas étonné »*. Il raconte qu'en juin, un journal marocain a publié des informations issues d'une conversation WhatsApp qu'il avait tenue avec deux personnes, et dont il n'avait parlé à personne. Sollicité, le Maroc affirme *« rejeter catégoriquement »* les *« allégations infondées »* faisant état de son usage de Pegasus. Le royaume nie être client de NSO Group. De son côté, NSO a affirmé ne pas connaître en temps réel ni contrôler l'usage fait par ses clients du logiciel : *« NSO ne pilote pas les systèmes qu'elle vend à ses clients gouvernementaux vérifiés, et n'a pas accès aux données des cibles de ses clients. »* Plus largement, NSO a contesté les conclusions des enquêtes du « Projet Pegasus », les qualifiant *« pour beaucoup de théories non corroborées »*.

DES CAUSES PAS TOUJOURS CLAIRES

Les journalistes marocains ne sont pas les seuls à intéresser les services de renseignement du royaume chérifien. Une trentaine de journalistes et de patrons de médias français figurent sur la liste des cibles de Pegasus, dans des rédactions aussi variées que *Le Monde*, *Le Canard enchaîné*, *le Figaro* ou encore l'AFP et France Télévisions. A plusieurs reprises, le consortium Forbidden Stories et le Security Lab d'Amnesty International ont pu techniquement déterminer que l'infection avec Pegasus avait été couronnée de succès. C'est le cas notamment d'Edwy Plenel, le fondateur de *Mediapart*, de Dominique Simonnot, ancienne enquêtrice du *Canard enchaîné* et désormais contrôleuse générale des lieux de privation de liberté – elle a annoncé sur Franceinfo vouloir déposer une plainte –, mais aussi d'une journaliste du *Monde*, qui n'a pas souhaité rendre publique son infection.

Dans certains cas, la cause de l'attaque semble claire : Edwy Plenel a été visé peu après avoir publiquement critiqué la répression policière des manifestations du Rif, comme l'a confirmé une analyse menée par le Security Lab d'Amnesty International. En juin 2019, alors qu'il participait à une table ronde lors d'un festival à Essaouira, M. Plenel se souvient être *« intervenu pour manifester qu*['il] *n'allai*[t] *pas* [s]*e censurer parce qu*['il] *était*[t] *au Maroc ;* [il a] *évoqué le sort du Hirak, du Rif, et la répression dont les manifestations populaires faisaient l'objet »*. Pour le fondateur de *Mediapart*, cette intervention a pu servir de déclencheur, mais ce sont surtout *« nos confrères marocains, et de fait l'indépendance du* Desk [média qui était partenaire de *Mediapart*] *»* qui étaient visés. Il compte déposer plainte.

EDWY PLENEL A ÉTÉ VISÉ PEU APRÈS AVOIR PUBLIQUEMENT CRITIQUÉ LA RÉPRESSION POLICIÈRE DES MANIFESTATIONS DU RIF

Un téléphone d'une autre journaliste de *Mediapart*, Lenaïg Bredoux, a aussi été infecté. Spécialiste des violences sexuelles, thématique parfois instrumentalisée au Maroc contre des voix critiques du pouvoir, Mme Bredoux avait aussi écrit, en 2015, une série d'articles sur le patron de la DGST marocaine, Abdellatif Hammouchi. A l'époque, le chef du principal service de renseignement marocain était à la fois visé par une plainte en France pour complicité de torture, et pressenti pour être décoré par la République française pour sa collaboration à la lutte antiterroriste.

Un autre patron de média, Bruno Delport, directeur de la radio TSF Jazz (groupe Combat, propriété de Matthieu Pigasse, actionnaire à titre individuel du *Monde*), a aussi été visé par l'utilisateur marocain de Pegasus. M. Delport est aussi président du conseil d'administration de Solidarité Sida, une ONG qui a développé des programmes de prévention auprès des travailleuses du sexe au Maroc.

Si les services marocains semblent avoir majoritairement visé des journalistes travaillant pour des rédactions étiquetées à gauche ou au centre, les médias de droite n'ont pas été épargnés pour autant. Le Maroc a entré dans l'outil de NSO un numéro de téléphone aujourd'hui désactivé mais auparavant attribué au polémiste Eric Zemmour, auteur en février 2019 sur le plateau de LCI d'une violente diatribe contre les migrants marocains, sans que l'on sache si les deux événements sont liés.

Dans d'autres cas, le raisonnement des espions marocains semble brumeux : la journaliste du *Monde* dont le téléphone a été infecté ne travaille sur aucun dossier lié de près ou de loin au Maroc, tout comme d'autres journalistes dont les numéros ont été sélectionnés par le client marocain de NSO. Il est possible qu'ils aient été visés principalement pour qu'on puisse accéder à leur carnet d'adresses – et acquérir ainsi les numéros d'autres cibles. ■

DAMIEN LELOUP

Du Mexique à l'Inde, une obsession de surveillance commune

L'espionnage de la presse n'est pas l'apanage des pays autocratiques comme l'Azerbaïdjan. Des démocraties utilisent aussi Pegasus à cette fin

Azerbaïdjan, Togo, Bahreïn, Mexique : tous ces utilisateurs de Pegasus, et bien d'autres, ont en commun de viser des journalistes avec le puissant logiciel espion israélien. Depuis des années, des organisations comme Amnesty International et Reporters sans frontières (RSF) dénoncent l'utilisation de logiciels de ce type contre eux.

Les révélations du « Projet Pegasus » montrent que l'espionnage des journalistes ne concerne pas que les pays autocratiques, comme l'Azerbaïdjan. Des démocraties aussi surveillent des journalistes d'investigation, au Mexique ou en Inde, et même en Europe, en Hongrie. Certains Etats, comme le Maroc, n'hésitent pas non plus à viser des journalistes étrangers. En France, les services marocains se sont ainsi intéressés aux téléphones de journalistes du *Monde*, de *Mediapart*, de France Télévisions ou de Radio France, pour ne citer qu'une petite partie des cibles.

Les révélations du « Projet Pegasus » sont les toutes dernières d'une longue liste d'attaques contre des journalistes, commises grâce au logiciel espion de NSO Group. De précédentes enquêtes avaient déjà montré que des dizaines de collaborateurs de la presse mexicaine avaient été espionnés par ce biais.

Plusieurs lignes de défense

En 2020, des analyses techniques menées par les experts du Citizen Lab de l'université de Toronto, au Canada, montraient ainsi que trente-six journalistes et cadres d'une filiale de la chaîne de télévision qatarie Al-Jazira avaient été attaqués par Pegasus.

La même année, Amnesty International démontrait que le téléphone du journaliste marocain Omar Radi avait lui aussi été infecté par le logiciel espion.

Confrontée à ces usages illégaux de son logiciel, NSO Group a, au fil des années, adopté plusieurs lignes de défense, avançant tout à la fois que chaque client est responsable de la bonne utilisation de son logiciel, et que des procédures rigoureuses de contrôle et d'audit interne étaient conduites pour éviter, notamment, que des journalistes soient ciblés illégalement.

Après l'assassinat du chroniqueur et dissident saoudien Jamal Khashoggi au consulat d'Arabie saoudite, à Istanbul, alors que Pegasus était soupçonné d'avoir été utilisé par les autorités du royaume pour traquer ce dernier, le PDG de NSO Group, Shalev Hulio, avait vivement nié toute implication. Un client qui utiliserait Pegasus pour autre chose que la lutte contre le crime et le terrorisme risquerait une *« sanction immédiate, décisive et sans compromis »* de la part de NSO, affirmait-il.

Pratique régulière

L'analyse des données, partagées par Forbidden Stories et Amnesty International avec les seize médias partenaires du « Projet Pegasus », montre clairement que les exploitations du logiciel espion contre des journalistes ne sont pas des accidents.

Pire, la pratique est systématique, régulière, et concerne, à des niveaux de gravité divers, tous les clients sur lesquels les médias du « Projet Pegasus » ont enquêté. Si cette pratique est interdite et sanctionnée par NSO, ses clients ne semblent pas le savoir – ou sont confiants dans le fait que leurs chances d'être punis pour ce mésusage sont extrêmement faibles. ■

JULIEN BOUISSOU

L'investigation prise pour cible en Azerbaïdjan

Intimidation, divulgation de photos intimes et procédure judiciaire… Une enquêtrice en liberté conditionnelle raconte son calvaire

C'est dur. J'ai appris hier que mon téléphone avait été infecté, et j'ai passé la nuit à me demander ce que j'avais fait avec. Je me souviens d'avoir pris des photos de mes proches, dont un à l'hôpital après une opération, et maintenant je me sens coupable. Coupable d'avoir envoyé des messages, coupable pour mes sources qui m'ont envoyé des messages sur des applis sécurisées et qui ne savaient pas que mon téléphone était infecté. Ce n'est pas juste moi, ce sont mes sources, mes collègues, les personnes qui m'ont confié leurs secrets, qui sont touchés. » Khadija Ismayilova est journaliste d'investigation en Azerbaïdjan, un pays classé 167e sur 180 par Reporters sans frontières (RSF), dans son classement mondial de la liberté de la presse 2020.

Infections répétées

Autrice de plusieurs investigations remarquées, sur la corruption du régime, elle a publié des enquêtes mettant directement en cause le président azerbaïdjanais, Ilham Aliev. Et notamment son utilisation de sociétés offshore pour dissimuler une partie de sa fortune, dans le cadre des « Panama Papers ». Le téléphone de Mme Ismayilova a été infecté par Pegasus à de multiples reprises, tout au long de l'année 2019, a confirmé une analyse du téléphone menée par le Security Lab d'Amnesty International, qui a étudié plusieurs dizaines de téléphones touchés par le logiciel. Plus de vingt autres journalistes azerbaïdjanais ont été sélectionnés par le régime comme potentielles cibles de Pegasus, comme le montre l'analyse des données auxquelles Forbidden Stories a eu accès.

L'Azerbaïdjan n'a pas attendu l'arrivée de NSO Group pour mettre ses journalistes sous surveillance. Mme Ismayilova en a directement fait les frais : après la publication d'une enquête sur la fortune du président, en 2011, la journaliste avait découvert une caméra dans sa chambre. L'année suivante, des photos intimes, visiblement filmées par cette caméra, lui avaient été envoyées, assorties de menaces – elles seront ensuite publiées en ligne.

Elle est la cible d'une nouvelle campagne de harcèlement virulente en 2014, qui culminera dans une procédure judiciaire l'accusant d'avoir fraudé le fisc pour le compte de son employeur principal, Radio Free Europe – un média au statut associatif financé par le département d'Etat américain, qui ne gagne pas d'argent et ne peut donc frauder.

Condamnée à sept ans de prison, elle a été placée en liberté conditionnelle en 2015, après une vive campagne internationale demandant sa libération.

« Méprisable et haineux »

Frappée d'une interdiction de sortie du territoire, elle a finalement pu se rendre en Turquie, au printemps 2021, où plusieurs rédactions du consortium Forbidden Stories ont pu l'interviewer. « *Je suis en colère contre le gouvernement azerbaïdjanais, je suis en colère contre le gouvernement* [israélien] *qui autorise la vente de ce genre d'outils à des régimes comme celui d'Aliev. C'est méprisable, c'est haineux* », dit-elle.

Pour autant, « *il est vital que les journalistes continuent leur travail* [en Azerbaïdjan], *qu'il y ait des exemples de journalistes qui ne s'arrêtent pas malgré les menaces*, estime-t-elle. *C'est comme une guerre. Si vous quittez votre tranchée, votre assaillant s'y engouffrera. Il faut tenir la position, coûte que coûte, sinon vous aurez de moins en moins d'espace, jusqu'au moment où vous ne pourrez même plus respirer* ». ■

FORBIDDEN STORIES, OCCRP (ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT) ET « SÜDDEUTSCHE ZEITUNG »

En Inde, la presse sous l'œil du régime de Narendra Modi

Depuis 2016, une trentaine de journalistes indiens ont été espionnés à travers leurs smartphones grâce au logiciel de NSO

Le premier ministre indien, Narendra Modi, qui n'a organisé aucune conférence de presse avec questions depuis son élection, en 2014, fuit les journalistes tout en les surveillant de très près. Les agences de sécurité du pays lui en donnent en tout cas la possibilité grâce au logiciel Pegasus. L'Etat indien a sélectionné pour une éventuelle mise sous surveillance au moins une trentaine de journalistes indiens à partir de 2017. Contacté par le consortium de 17 médias, dont *Le Monde*, le gouvernement indien dément. « *L'engagement en faveur de la liberté d'expression comme droit fondamental est une pierre angulaire du système démocratique indien* », affirme-t-il avant d'ajouter : « *Prétendre que le gouvernement surveille certaines personnes en particulier ne repose sur aucune base concrète ni vérité.* »

Les analyses du Security Lab d'Amnesty International confirment pourtant que les téléphones de plusieurs journalistes indiens ont été infectés par Pegasus. Siddharth Varadarajan, cofondateur du site d'information indépendant *The Wire*, a été infecté par Pegasus entre le 4 avril 2018 et le 20 juillet 2018, peu après qu'il eut publié, à l'été 2017, une enquête sur les affaires douteuses du fils d'Amit Shah, alors dirigeant du parti au pouvoir, le BJP, devenu plus tard le puissant ministre de l'intérieur de M. Modi. Est-ce la raison pour laquelle il a été surveillé ? Probablement, mais il n'en est pas certain : « *Le problème, c'est justement que l'on ne sait pas pourquoi on est surveillé.* »

L'un des espionnés explique au *Monde* ne pas être surpris. Il se souvient de cet exercice de routine, avant chaque rencontre informelle avec un ministre de M. Modi : un assistant prenait les smartphones de ses visiteurs dans une pièce spécifique où retentissait une forte musique. Le ministre en question ignorait sans doute que le logiciel Pegasus ne permet pas seulement d'écouter les conversations, mais aussi de suivre la localisation.

Le journaliste d'investigation Paranjoy Guha Thakurta, ancien rédacteur en chef de la revue universitaire *Economic and Political Weekly*, a une petite idée de la raison pour laquelle il a été surveillé. Il enquêtait sur de puissants hommes d'affaires proches de M. Modi, dont Mukesh Ambani, l'homme le plus riche d'Asie à la tête du conglomérat Reliance Industries, et Gautam Adani dirigeant de l'entreprise éponyme qui a bénéficié de nombreuses concessions de l'Etat pour exploiter des ports et des aéroports.

Foyers de contestation

Les agences de sécurité indiennes s'intéressent aussi à ceux qui sont en contact régulier avec des diplomates ou des militaires. Prem Shankar Jha, un éditorialiste de 82 ans souvent invité à l'ambassade de France, à New Delhi, pour partager ses analyses politiques et géopolitiques – où il a été décoré chevalier de la Légion d'honneur en décembre 2017 –, a ainsi été sélectionné pour une éventuelle mise sous surveillance. Sushant Singh, un journaliste du quotidien *The Indian Express* est sous surveillance lorsqu'il publie, en août 2018, un article mentionnant que le groupe partenaire de Dassault en Inde, dirigé par Anil Ambani, a coproduit, en 2016, un film de Julie Gayet, alors compagne de François Hollande.

L'Etat indien s'inquiète également des foyers de contestation allumés par les médias régionaux. Il a sélectionné pour une éventuelle mise sous surveillance Jaspal Singh Heran, rédacteur en chef du quotidien en pendjabi *Pehredar*, lu par la communauté Sikh, au second semestre 2019. Il n'exclut pas une manœuvre du Rashtriya Swayamsevak Sangh (RSS), l'organisation d'extrémistes hindous dont est issu M. Modi et qui est très influente au sommet de l'Etat : « *Le RSS est en colère contre nous, ils veulent instaurer une nation hindoue, or la communauté sikh est un groupe ethnique, religieux et social qui ne fait pas partie de l'hindouisme.* » Cette surveillance des journalistes devrait précipiter un peu plus la dégringolade de l'Inde au classement mondial de la liberté de la presse, établi par RSF. Elle est passée au 142e rang sur 180 en 2020. ■

JULIEN BOUISSOU

Au moins vingt-cinq reporters mexicains sur les listes

Parmi les numéros ciblés figurent les grandes rédactions du pays, ainsi qu'un correspondant du « New York Times »

Le 18 juin 2017, le *New York Times* publiait une enquête explosive. Le quotidien américain révélait, grâce à des informations de l'ONG R3D et des chercheurs du Citizen Lab de Toronto, que le gouvernement d'Enrique Peña Nieto avait utilisé le logiciel espion Pegasus de NSO Group pour pirater les téléphones de défenseurs des droits de l'homme et de journalistes, dont l'équipe d'enquêteurs du journal *Proceso*.

Trois semaines avant cette publication, une agence gouvernementale mexicaine, dont plusieurs éléments indiquent qu'il s'agit du centre d'enquête et de sécurité nationale (Cisen, principal service de renseignement mexicain), avait entré dans les systèmes de NSO Group le numéro d'Azam Ahmed, à l'époque correspondant du *New York Times* au Mexique, révèlent ce 18 juillet les rédactions du « Projet Pegasus ». On ignore si le téléphone du journaliste a été infecté.

Les numéros d'au moins vingt-cinq journalistes mexicains, travaillant pour la quasi-totalité des grands médias du pays, apparaissent dans la liste de plus de 50 000 numéros de téléphone sélectionnés par des clients de NSO, que Forbidden Stories et Amnesty International ont partagée avec dix-sept rédactions.

Au Mexique, en 2016 et 2017, les attaques de Pegasus se faisaient au moyen de SMS contenant des liens piégés, sur lesquels l'utilisateur était incité à cliquer. Plus récemment, NSO a développé pour son logiciel des attaques dites « *zero clic* », qui ne nécessitent plus aucune action de la part de la cible pour que le logiciel espion s'installe sur son appareil.

Cette violence contre la presse est endémique au Mexique, où l'organisation Articulo 19 a enregistré quarante-sept assassinats de journalistes durant les six années de mandat d'Enrique Peña Nieto. Le 2 mars 2017, Cecilio Pineda Brito, journaliste dans la région de Tierra Caliente, dans l'Etat de Guerrero, était tué par deux hommes à moto, alors qu'il attendait sa voiture dans une station de lavage.

La liste des numéros sélectionnés par les clients de NSO montre que, début 2017, une agence gouvernementale présentant les caractéristiques de la Sedena (secrétariat à la défense nationale) y avait ajouté celui du portable de Cecilio Pineda Brito. Faute d'avoir pu mener des analyses détaillées sur le téléphone du défunt, il est impossible de confirmer s'il a été infecté. Peu avant son assassinat, le journaliste avait accusé publiquement le gouverneur de la région de protéger un groupe criminel dirigé par un mafieux surnommé « El Tequilero ».

Cecilio Pineda Brito recevait régulièrement des menaces de mort sur les réseaux sociaux, et avait déjà été visé par une attaque en septembre 2015. Lors de la dernière conversation téléphonique avant sa mort, avec l'organisme chargé de sa protection, il estimait que d'éventuels assaillants « [ne savaient] *pas où* [il] *vi*[vait], [il] *chang*[eait] *de lieu régulièrement* ». Les enquêteurs ont conclu que l'exécution du journaliste avait été ordonnée par « El Tequilero » – lui-même mort assassiné en 2019.

Les numéros des proches visés

La surveillance de Cecilio Pineda Brito rappelle celle du journaliste et fondateur du *Riodoce* Javier Valdez Cardenas, tué en plein jour, le 15 mai 2017, à Culiacan. Dans les semaines qui avaient suivi son assassinat, une agence gouvernementale, vraisemblablement la Cisen, a ajouté à la liste des numéros éventuellement ciblés par Pegasus ceux de sa veuve et de deux hauts cadres de sa rédaction.

Les données consultées par les rédactions du « Projet Pegasus » éclairent également les précédentes révélations du *New York Times* sur la surveillance de journalistes de *Proceso*, l'un des principaux hebdomadaires mexicains, classé à gauche. Ont également été trouvés dans la liste consultée par les journalistes du « Projet Pegasus » des numéros de téléphone utilisés par la sœur de la journaliste d'investigation Carmen Aristegui (qui a participé à cette enquête), ainsi que par plusieurs personnes travaillant avec elle. ■

MATHIEU TOURLIÈRE AVEC FORBIDDEN STORIES ET « ARISTEGUI NOTICIAS »

En Hongrie, la société civile sous contrôle

Hommes d'affaires et patrons de presse figurent parmi les 300 numéros ciblés pour le compte de Budapest

BUDAPEST - *envoyé spécial*

Les révélations du « Projet Pegasus » ne vont pas rassurer ceux qui s'inquiètent des dérives du premier ministre nationaliste, Viktor Orban, en matière d'Etat de droit. *Le Monde* et ses seize médias partenaires peuvent de fait affirmer, grâce aux données mises à disposition par les organisations Forbidden Stories et Amnesty International et au témoignage d'un ancien employé de NSO Group, que la Hongrie a eu recours aux services particulièrement intrusifs de la société israélienne pour mettre sous surveillance des journalistes, des propriétaires de médias et des avocats, tous connus pour être des critiques du pouvoir de M. Orban.

Parmi les plus de trois cents numéros de téléphone sélectionnés comme cibles potentielles par la Hongrie, *Le Monde* et ses partenaires ont pu identifier au moins cinq journalistes. Il s'agit notamment d'Andras Szabo et de Szabolcs Panyi, journalistes reconnus du site d'investigation *Direkt36*. Ces dernières années, ce petit site a multiplié les révélations dérangeantes sur l'enrichissement des proches de Viktor Orban ou sur les relations que celui-ci entretient avec la Russie et la Chine. *« J'ai toujours su que je pouvais être surveillé, mais là, c'est une surveillance avec le meilleur logiciel du monde »*, dénonce M. Panyi, 35 ans, qui a découvert qu'entre avril et décembre 2019 son téléphone a été infecté près d'une vingtaine de fois.

Benyamin Nétanyahou, alors premier ministre d'Israël, et son homologue hongrois, Viktor Orban, avant une conférence de presse à Budapest, le 19 juillet 2017. AKOS STILLER/BLOOMBERG VIA GETTY IMAGES

Un dîner très préoccupant

A cette époque, M. Panyi enquêtait notamment sur le transfert du siège de la Banque internationale d'investissement de Moscou à Budapest. L'infection de son appareil, plusieurs fois concomitante à l'envoi de questions au gouvernement, et de celui de son collègue Andras Szabo a été confirmée par les analyses techniques de leurs appareils par les experts du Security Lab d'Amnesty International.

Deux autres reporters hongrois, travaillant sur des sujets relatifs à la criminalité et au terrorisme, ainsi que l'ex-femme de l'un d'entre eux, ont aussi été désignés comme cibles potentielles. Parmi les autres numéros identifiés figure enfin celui d'un photographe qui travaillait comme fixeur pour un journaliste étranger enquêtant sur la même banque russe.

Pegasus est connu comme un logiciel particulièrement intrusif parce qu'il peut aspirer, en toute discrétion, e-mails, liste de contacts, localisation géographique, SMS, appels téléphoniques, documents, photographies… NSO assure que son usage doit être réservé à la lutte contre le terrorisme et le crime organisé. Mais si la liste de numéros contient ceux de proches notoires du milieu criminel hongrois, la présence d'autres personnalités pose question. Figurent ainsi les numéros du fils et de l'avocat de Lajos Simicska, un riche homme d'affaires anciennement très proche de M. Orban, brusquement devenu l'un de ses ennemis.

Le Monde et ses partenaires ont aussi retrouvé le numéro de Zoltan Varga, propriétaire de Central Media Group, le dernier groupe de médias indépendant du pays.

> **« J'AI TOUJOURS SU QUE JE POUVAIS ÊTRE SURVEILLÉ, MAIS LÀ, C'EST UNE SURVEILLANCE AVEC LE MEILLEUR LOGICIEL DU MONDE »**
>
> **SZABOLCS PANYI**
> journaliste du site d'investigation Direkt36

Cet homme d'affaires, qui dénonce depuis des mois les intimidations exercées par le pouvoir pour qu'il vende ses titres, a été désigné comme cible potentielle autour d'un dîner organisé sur la terrasse de sa villa, sur les collines de Budapest, le 5 juin 2018, quelques semaines après la troisième victoire d'affilée de M. Orban aux législatives. *« Nous avons juste discuté de l'idée de créer un think tank pour travailler par exemple sur la corruption »*, se remémore, trois ans plus tard, celui qui a fait fortune en investissant notamment dans la compagnie aérienne hongroise à bas coût Wizz Air. *« C'était juste une discussion amicale, pas un coup d'Etat »*, assure M. Varga, qui détient aussi le plus grand site d'information indépendant hongrois, *24.hu*.

« Tout le monde avait son téléphone avec soi », se souvient précisément l'homme d'affaires, interrogé par nos partenaires du *Guardian* et du site d'investigation hongrois *Direkt36*. Or, le « Projet Pegasus » a non seulement retrouvé le numéro de M. Varga, mais également ceux de six autres convives, tous d'influents Hongrois connus pour être critiques de M. Orban, dans la liste des cibles désignées autour de ce 5 juin. Les analyses menées par les équipes d'Amnesty International sur le seul téléphone des convives compatible et encore accessible ont confirmé qu'il avait été infecté entre le 1er juin et le 10 juillet 2018.

Contacté par *Le Monde* et ses partenaires, le gouvernement hongrois a dit *« ne pas être au courant d'une quelconque collecte de données »* et avoir *« toujours agi et continué d'agir conformément à la loi en vigueur »*. Chargée d'approuver les écoutes pour « sécurité nationale », la ministre de la justice, Judit Varga, avait qualifié de *« provocation »* une question sur d'éventuelles écoutes de journalistes posée au détour d'une interview menée dans ses bureaux en juin.

« Pratique communiste »

Selon les statistiques officielles, la ministre est amenée à autoriser plus de mille écoutes par an, ce chiffre incluant potentiellement celles effectuées par le logiciel Pegasus, mais aussi les écoutes téléphoniques plus classiques. *« Il y a tellement de dangers partout pour l'Etat »*, avait-elle justifié.

En vertu du cadre légal hongrois, son ministère peut autoriser des écoutes pour quatre-vingt-dix jours sans aucun contrôle ; une pratique dénoncée par un arrêt de la Cour européenne des droits de l'homme de 2016.

Si ces manquements ne datent pas de l'arrivée au pouvoir de Viktor Orban, celui qui vient d'être désigné « ennemi de la liberté de la presse » par Reporters sans frontières peut avoir accès à un niveau de surveillance jamais vu en Hongrie. Jusqu'ici, personne ne savait qu'il avait conclu un contrat avec NSO. L'accès à son service très spécial semble d'ailleurs avoir été négocié directement avec l'ancien premier ministre israélien, Benyamin Nétanyahou, très proche politiquement de M. Orban. L'usage commercial de Pegasus par les Hongrois a débuté en février 2018, pile au moment de la visite en Israël de Jozsef Czukor, alors conseiller en chef pour la sécurité et la politique internationale de M. Orban. Il avait été reçu par le premier ministre israélien en personne.

La Hongrie n'est pas le seul pays de l'Union européenne à utiliser les services de NSO, mais elle est le seul pour lequel nous avons pu identifier des journalistes, des avocats ou un militant, comme Adrien Beauduin. Cet ancien étudiant belgo-canadien de l'Université d'Europe centrale, établissement fondé et financé par le milliardaire américain d'origine hongroise George Soros, avait été arrêté, en décembre 2018, pour « rébellion contre les forces de l'ordre », lors d'une manifestation contre le pouvoir. Son téléphone a fait l'objet d'une tentative d'intrusion quelques jours après son arrestation, mais les analyses effectuées sur son appareil n'ont pas pu confirmer si elle avait été effective. *« C'est tout à fait illégitime de mettre sous surveillance des personnes prenant part à des mouvements sociaux qui n'ont pas montré l'intention d'employer des méthodes illégales »*, dénonce celui qui est toujours poursuivi pour avoir porté un cutter sur lui, assurant *« avoir seulement exercé son droit démocratique »* de manifestation. *« Une ligne rouge a été franchie. Surveiller des civils, c'est clairement une pratique associée au passé communiste »*, affirme M. Panyi, qui doit désormais prendre des précautions de sécurité ultrarenforcées pour rencontrer ses sources. ■

JEAN-BAPTISTE CHASTAND

Dans les coulisses de la traque d'un logiciel espion sophistiqué

Le mouchard Pegasus de NSO est en évolution constante, afin d'échapper à la vigilance d'experts tels que ceux d'Amnesty International

Comment démasquer les technologies de surveillance ? En se prêtant au jeu du chat et de la souris, comme le font une poignée d'experts en sécurité informatique qui traquent les traces techniques complexes laissées par un logiciel sophistiqué, Pegasus, qui déploie des efforts incommensurables pour masquer sa présence et se dérober. Le travail de fourmi mené par le consortium coordonné par Forbidden Stories sur ce mouchard, commercialisé par l'entreprise israélienne NSO Group, montre l'usage dévoyé et contraire au droit international qu'en font plusieurs Etats. Une enquête que l'entreprise NSO, contactée par le « Projet Pegasus », conteste, affirmant notamment que *« ces accusations sont pour beaucoup des théories non corroborées, qui jettent de sérieux doutes sur la crédibilité de vos sources, ainsi que sur le cœur de votre enquête »*.

Cet outil élusif, qui infecte les smartphones et en extrait une quantité massive d'informations, n'apparaît pas sur l'écran d'accueil des victimes, pas plus qu'il n'installe d'icônes ou ne produit de notifications. Pour les chercheurs d'Amnesty International, il a fallu approcher des activistes et journalistes ciblés et explorer de fond en comble les traces présentes sur leur téléphone. Des constatations techniques qui ont également permis de confirmer l'authenticité de la liste de numéros présélectionnés par des clients de NSO pour une éventuelle mise sous surveillance, que Forbidden Stories a consultée. Dans un long rapport technique publié dimanche 18 juillet, et revu par des pairs, Amnesty International détaille le fonctionnement de ce mouchard très sophistiqué.

Pegasus a été ausculté une première fois en 2016, par des chercheurs du laboratoire canadien Citizen Lab. Un opposant émirati, nommé Ahmed Mansoor, avait à l'époque reçu sur son iPhone un SMS suspect venant d'un numéro qu'il ne connaissait pas, et l'invitant à suivre un lien. Les experts en sécurité informatique qui lui ont prêté main-forte ont pu mettre en place un environnement sécurisé pour analyser ce lien. En cliquant dessus, on arrivait sur une page Internet contenant du code informatique exploitant des failles logicielles afin de forcer la sécurité de Safari, le navigateur Internet d'iOS, à télécharger et installer le logiciel espion.

En 2019, en fouillant le téléphone d'un journaliste marocain, les chercheurs d'Amnesty International ont pu découvrir des liens suspects vers lesquels la cible avait été redirigée, alors qu'elle cherchait à visiter un site Internet n'ayant rien à voir.

Des techniques similaires sont toujours utilisées, mais le dernier rapport d'Amnesty montre que les méthodes de NSO et de Pegasus évoluent. En observant sur les téléphones de victimes le fonctionnement d'iMessage, l'outil de messagerie d'Apple, ceux-ci ont découvert la méthode d'infection « zero click », apparue en 2019 : l'installation du mouchard a lieu sans que le propriétaire du téléphone fasse quoi que ce soit.

« Suivre les petits cailloux »

Dans son rapport, l'ONG détaille plusieurs méthodes « zero click », qui permettent à NSO d'installer son logiciel espion en toute discrétion sans que les cibles puissent se protéger.

« Les choses deviennent de plus en plus compliquées pour les utilisateurs. Il n'y a pas vraiment de signe visible les alertant que quelque chose est en train de se passer », explique Claudio Guarnieri, expert du Security Lab d'Amnesty International et coauteur du rapport, à Forbidden Stories.

C'est d'ailleurs parce que ces chercheurs ont minutieusement étudié de nombreuses attaques depuis plusieurs années, qu'ils parviennent à en repérer des similarités. Par exemple, un morceau de code malveillant, un processus nommé « msgacnted », retrouvé à la fois sur un téléphone ciblé en 2021 et sur un autre attaqué en 2019, à chaque fois par Pegasus.

Il en va de même pour les infrastructures et serveurs utilisés par NSO, et qu'Amnesty International et le Citizen Lab tentent de cartographier avec précision. Un logiciel de ce type a en effet besoin de pouvoir interagir avec des serveurs et des sites Internet, afin de pouvoir recevoir ou exfiltrer des données. Les chercheurs en ont dévoilé plusieurs centaines en quelques années.

Ce travail, qui s'apparente à un combat de David contre Goliath, ne passe pas inaperçu et a, à plusieurs reprises, forcé NSO à réparer des erreurs, ce alors que cette puissante entreprise dispose de plus de ressources qu'un petit groupe d'experts au sein de laboratoires et d'ONG. *« A chaque fois que des détails techniques sur les outils d'espionnage de NSO sont publiés soit par* [le Citizen Lab] *soit par Amnesty ou quelqu'un d'autre, NSO les analyse de très près et réagit. (…) Ils peuvent, comme en 2018, fermer leurs serveurs et en lancer d'autres, ou changer des aspects de leur logiciel »*, raconte Bill Marczak, chercheur au Citizen Lab, dans une interview à Forbidden Stories. Les nouvelles découvertes par les chercheurs et transmises à Apple devraient de nouveau contraindre l'entreprise à réagir. ■

FLORIAN REYNAUD