Maroc. Des défenseurs des droits humains ciblés par un logiciel espion de NSO Group

○ Résumé

- Amnesty International a découvert des attaques informatiques ciblées contre deux défenseurs des droits humains marocains de premier plan menées à l'aide du logiciel espion Pegasus de NSO Group. D'après nos recherches, ces attaques ciblées durent au moins depuis 2017. Elles ont été menées au moyen de SMS contenant des liens malveillants qui, si la victime cliquait dessus, tenteraient d'exploiter son dispositif mobile et d'y installer le logiciel espion Pegasus de NSO Group.
- Outre les SMS, nous avons identifié ce qui semble être des attaques par injection de trafic réseau contre le réseau mobile d'un défenseur des droits humains visant elles aussi à installer un logiciel espion. Amnesty International soupçonne NSO Group d'être également à l'origine de ces attaques par injection de trafic réseau.
- Ces attaques informatiques ciblées contre deux défenseurs des droits humains marocains sont symptomatiques d'un phénomène plus large de représailles exercées par les autorités marocaines contre les personnes qui défendent les droits humains et contre les voix dissidentes. Cette situation rend de plus en plus difficile l'exercice des droits à la liberté d'expression, d'association et de réunion pacifique des défenseur·e·s des droits humains et des militant·e·s.

○ Introduction

Amnesty International a découvert que, depuis octobre 2017 au moins, des défenseurs des droits humains du Maroc ont été pris pour cible par « Pegasus », le logiciel espion tristement célèbre produit par l'entreprise israélienne « NSO Group ». Ce rapport dévoile comment ce logiciel a été utilisé pour cibler illégalement deux défenseurs des droits humains marocains de premier plan, qui ont déjà fait l'objet de représailles de la part de l'État pour s'être exprimés ouvertement sur la situation des droits humains dans le pays. Amnesty International est en mesure de révéler que les deux personnes prises pour cible sont **Maati Monjib**, universitaire et militant travaillant sur des questions de liberté d'expression, et **Abdessadak El Bouchattaoui**, avocat spécialiste des droits humains impliqué dans la défense de manifestants pour la justice sociale du mouvement du Hirak, qui s'est déroulé dans la région du Rif en 2016 et 2017.

Ces révélations sont particulièrement importantes dans un contexte où les autorités marocaines ont de plus en plus recours à des dispositions répressives du Code pénal et de la législation relative à la sécurité pour pénaliser et discréditer les défenseur·e·s des droits humains et les militant·e·s pour avoir exercé leurs droits à la liberté

d'expression, d'association et de réunion pacifique. Les personnes qui défendent les droits humains au Maroc sont harcelées, intimidées et emprisonnées. Ce rapport révèle que, depuis 2017 au moins, les autorités ont également utilisé un logiciel espion de NSO Group pour réduire encore davantage l'espace accordé aux actions en faveur des droits humains en ciblant les défenseurs des droits humains.

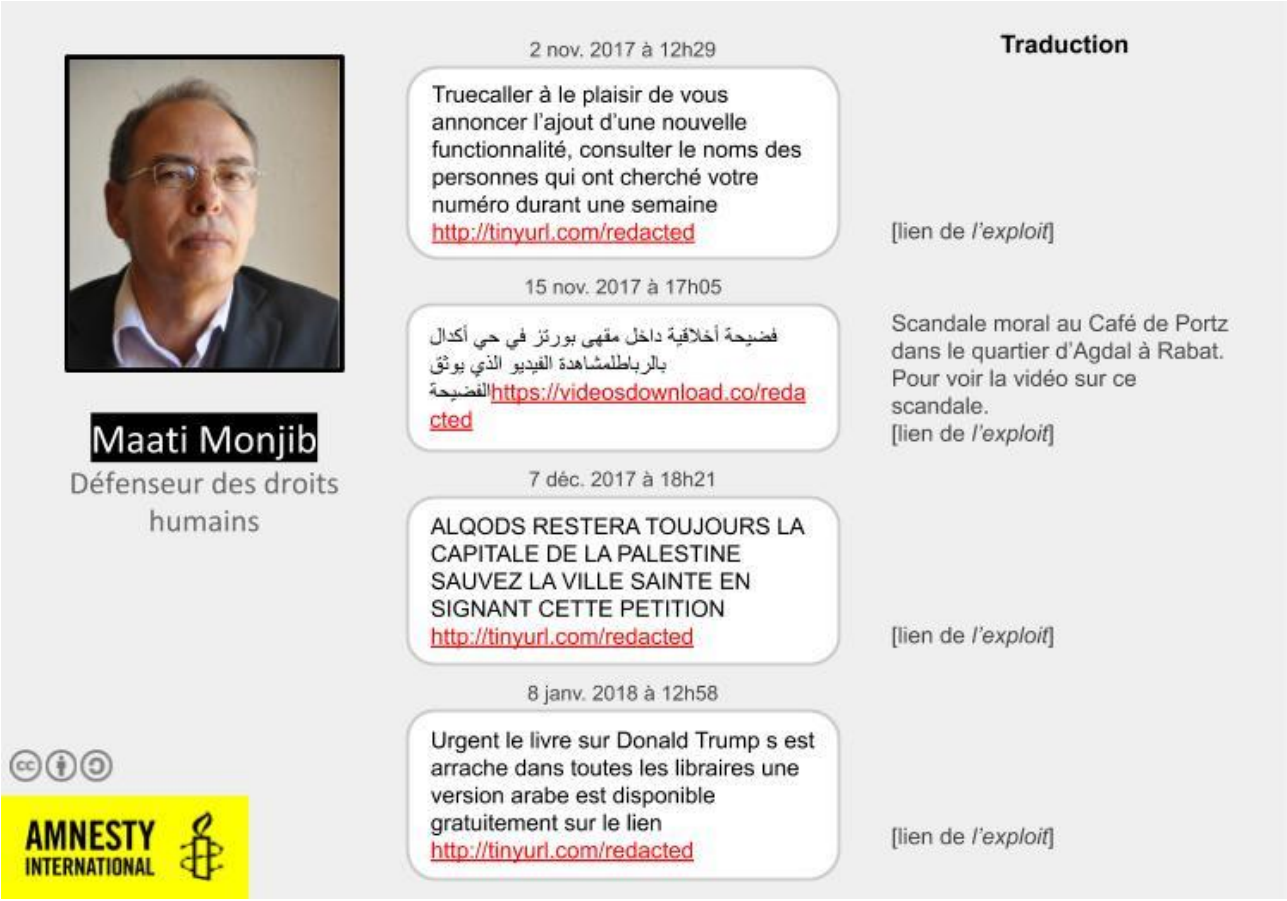
Maati Monjib

Maati Monjib, 57 ans, est historien et éditorialiste, cofondateur de l'ONG Freedom Now (consacrée à la protection des droits des journalistes et des écrivains) et cofondateur et membre dirigeant de l'Association marocaine pour le journalisme d'investigation (AMJI). C'est un important défenseur de la liberté d'expression au Maroc. En 2015, selon des documents officiels du tribunal, les autorités du Maroc l'ont accusé, lui et quatre autres personnes, d'« atteintes à la sûreté intérieure de l'État » par le biais d'une « propagande » de nature à « ébranler la fidélité que les citoyens doivent à l'État et aux institutions du peuple marocain » (article 206 du Code pénal). S'ils sont déclarés coupables, ils pourraient se voir infliger une peine allant jusqu'à cinq ans d'emprisonnement. Ces accusations reposent sur le simple fait qu'ils ont encouragé l'utilisation d'une application mobile de journalisme citoyen protégeant la confidentialité des utilisateurs. Le procès est en cours. Maati Monjib a déjà fait une grève de la faim pour protester contre les restrictions à sa liberté de mouvement. Amnesty International exhorte les autorités marocaines à abandonner les poursuites contre Maati Monjib et ses coaccusés.

Depuis 2015, Maati Monjib pense qu'il fait l'objet d'une surveillance numérique menée par les autorités marocaines. Cette surveillance a affecté ses activités militantes et sa vie quotidienne. Le fait de devoir sans cesse analyser ce qu'il devrait ou ne devrait pas dire dans ses communications numériques le soumet à une forte pression psychologique.

> **« Je dois constamment analyser les conséquences de ce que je dis et le risque que cela donne lieu à des accusations diffamatoires à mon encontre. Cela s'applique même à des considérations très terre-à-terre comme l'organisation de réunions ou un dîner en ville. »**
>
> *Maati Monjib, défenseur des droits humains marocain, août 2019*

Les craintes de Maati Monjib se sont avérées fondées. Amnesty International l'a rencontré et a vérifié si ses appareils montraient des traces de ciblage. **Nous avons découvert qu'il avait reçu à plusieurs reprises des SMS malveillants contenant des liens pointant vers des sites associés au logiciel espion Pegasus de NSO Group.**



Abdessadak El Bouchattaoui

Abdessadak El Bouchattaoui est avocat et défenseur des droits humains. Il fait partie de l'équipe d'avocats qui défendent les personnes incarcérées pour avoir participé aux manifestations pour la justice sociale du Hirak, dans la région du Rif, en 2016 et 2017. En février 2017, un tribunal d'Al Hoceima l'a condamné à 20 mois de prison et à une amende pour avoir critiqué en ligne le recours à une force excessive de la part des autorités lors des manifestations. Il a été inculpé au titre de dispositions pénales répressives qui érigent en infraction l'exercice du droit à la liberté d'expression. Depuis le milieu de l'année 2018, Abdessadak El Bouchattaoui vit en France, où sa demande d'asile a été acceptée. Amnesty International appelle les autorités marocaines à annuler sa condamnation.

Depuis qu'il a commencé à défendre les manifestants du HirakEl-Rif, Abdessadak El Bouchattaoui était lui aussi à peu près certain d'être surveillé par l'État. Il nous a dit avoir été suivi à plusieurs reprises et que ses clients ont eux aussi été harcelés. Au cours de son procès, Abdessadak El Bouchattaoui a reçu des menaces de mort et sa famille a fait l'objet de manœuvres d'intimidation par téléphone. Cela a affecté son bien-être psychologique et il est devenu difficile pour lui d'exercer son travail. Abdessadak El Bouchattaoui soupçonnait depuis longtemps que ses communications numériques étaient surveillées. Ses soupçons sont maintenant définitivement

confirmés.

> **« Au Maroc, la surveillance se fait ouvertement et de manière éhontée. [C'est] une forme de punition. On ne peut pas agir librement. Vous faire soupçonner que vous êtes surveillé fait partie de leur stratégie, l'objectif est de vous donner l'impression d'être constamment sous pression. »**
> Abdessadak El Bouchattaoui, défenseur des droits humains marocain, août 2019

Après avoir vérifié si ses appareils montraient des indices de ciblage, Amnesty International a pu confirmer qu'Abdessadak El Bouchattaoui avait en effet été pris pour cible à plusieurs reprises par des SMS malveillants contenant des liens qui pointaient vers des sites associés au logiciel espion Pegasus de NSO Group.

Les messages contenant des liens malveillants lui ont été envoyés à l'époque où, selon ses souvenirs, le mouvement du Rif était à son apogée, puis durant la répression par les forces de sécurité marocaines qui s'en est suivie.

Dans son cas, les auteurs de l'attaque ont astucieusement conçu celle-ci pour qu'elle ressemble à un afflux de SMS indésirables envoyés automatiquement avec le même texte et présentant le lien malveillant comme un moyen de ne plus les recevoir. Détail intéressant, certains des liens malveillants commençaient avec une majuscule : « *Https://* » au lieu de « *http://* » et dans l'un des messages, un caractère manquait dans le lien, ce qui nous porte à croire que les attaquants ont tapé ces SMS

manuellement, puis qu'ils les ont envoyés depuis un numéro marocain.

○ Comment sait-on que le produit de NSO Group est utilisé ?

En juin 2018, Amnesty International a rassemblé des informations sur le ciblage d'une personne membre du personnel d'Amnesty International et d'une personne qui défendait les droits humains en Arabie saoudite. Ces ciblages étaient effectués à l'aide du logiciel Pegasus de NSO Group. Les SMS envoyés à ces deux personnes contenaient des liens dirigeant vers des sites Internet malveillants associés à NSO Group. Les SMS envoyés aux défenseurs des droits humains mentionnés dans ce rapport contiennent des liens similaires pointant vers la même infrastructure exposée sur Internet et attribuée à NSO.

Ces messages, désignés par le terme « Enhanced Social Engineering Message » (ESEM) dans un document confidentiel de NSO Group qui a été rendu public, cherchent à inciter les victimes à cliquer sur le lien, ce qui déclencherait une tentative d'exploitation du téléphone et l'installation silencieuse du logiciel espion Pegasus sur l'appareil.

Deux noms de domaine des liens envoyés à Maati Monjib et Abdessadek El Bouchattaoui, **stopsms[.]biz** et **infospress[.]com**, avaient déjà été identifiés et révélés par Amnesty International comme faisant partie de l'infrastructure d'exploitation de NSO Group. Nous avons en outre identifié un nom de domaine que nous ne connaissions pas : **hmizat[.]co**, qui semble vouloir se faire passer pour Hmizate, une entreprise marocaine de commerce en ligne. Un message contenant un lien avec ce nom de domaine présentait les mêmes caractéristiques que les SMS typiques de Pegasus. (Voir en annexe la liste complète des SMS identifiés.)

(Remarque : dans ce rapport, les noms de domaine et les liens sont brisés, par exemple en remplaçant les points par « [.] » ou « http » par « hxxp », afin d'éviter de cliquer dessus ou de les copier-coller accidentellement.)

Un autre nom de domaine que nous avons trouvé dans les SMS envoyés aux défenseurs des droits humains marocains, **revolution-news[.]co**, avait déjà été identifié par Citizen Lab dans le rapport "Hide and Seek: Tracking NSO Group's Spyware to Operations in 45 Countries" et associé à l'auteur malveillant surnommé « *ATLAS* » par Citizen Lab, qui le soupçonne d'être d'origine marocaine.

En conclusion, les noms de domaine et les caractéristiques des liens envoyés par SMS à Maati Monjib et Abdessadek El Bouchattaoui nous permettent de supposer que, si les victimes avaient cliqué dessus, cela aurait donné lieu à une tentative d'exploitation de leurs appareils et à l'infection de ceux-ci par le logiciel espion Pegasus de NSO Group, ce qui aurait permis aux attaquants de surveiller la totalité des

communications des victimes et d'autres données leur appartenant.

○ Des attaques par injection de trafic réseau mobile pour installer un logiciel espion ?

En analysant l'iPhone de Maati Monjib, qui, comme nous l'avons confirmé plus haut, était ciblé par des liens malveillants envoyés par SMS visant à installer le logiciel espion Pegasus de NSO Group, nous avons observé des traces suspectes qui semblent révéler des tentatives d'exploitation singulières.

En inspectant l'historique de navigation de Safari de Maati Monjib, nous avons découvert des consultations de liens suspects ne provenant pas de messages SMS ou WhatsApp.

Safari enregistre tout son historique de navigation dans une base de données SQLite stockée sur l'appareil (et pouvant être exportée grâce à une procédure de sauvegarde d'iTunes). Cette base de données conserve non seulement chacun des liens consultés, mais aussi l'origine et la destination de chaque visite. Cela nous permet de reconstituer les redirections et la chronologie des requêtes web.

Le 22 juillet, Maati Monjib a ouvert Safari et cherché à consulter Yahoo en tapant manuellement « yahoo.fr » dans la barre d'adresse. Le navigateur a d'abord tenté une connexion non chiffrée à http://yahoo.fr.

En temps normal, le navigateur aurait été immédiatement redirigé par Yahoo vers son site sécurisé via TLS à l'adresse https://fr.yahoo.com/. Mais l'historique de connexion indique que la page a immédiatement (en moins de trois millisecondes) redirigé le navigateur vers un site d'aspect très suspect :

```
hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz
```

Cette visite a été suivie d'une redirection vers le même domaine, avec des paramètres additionnels :

```
hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz#0486347
8734328748598247485301272499805471849442328 6
```

Ce genre de redirection n'est possible que lorsque la requête n'est pas chiffrée ni protégée par un protocole de sécurité de la couche transport (TLS, c'est-à-dire le *https://* que l'on voit parfois dans les liens), ce qui était le cas avec *http://yahoo.fr*.

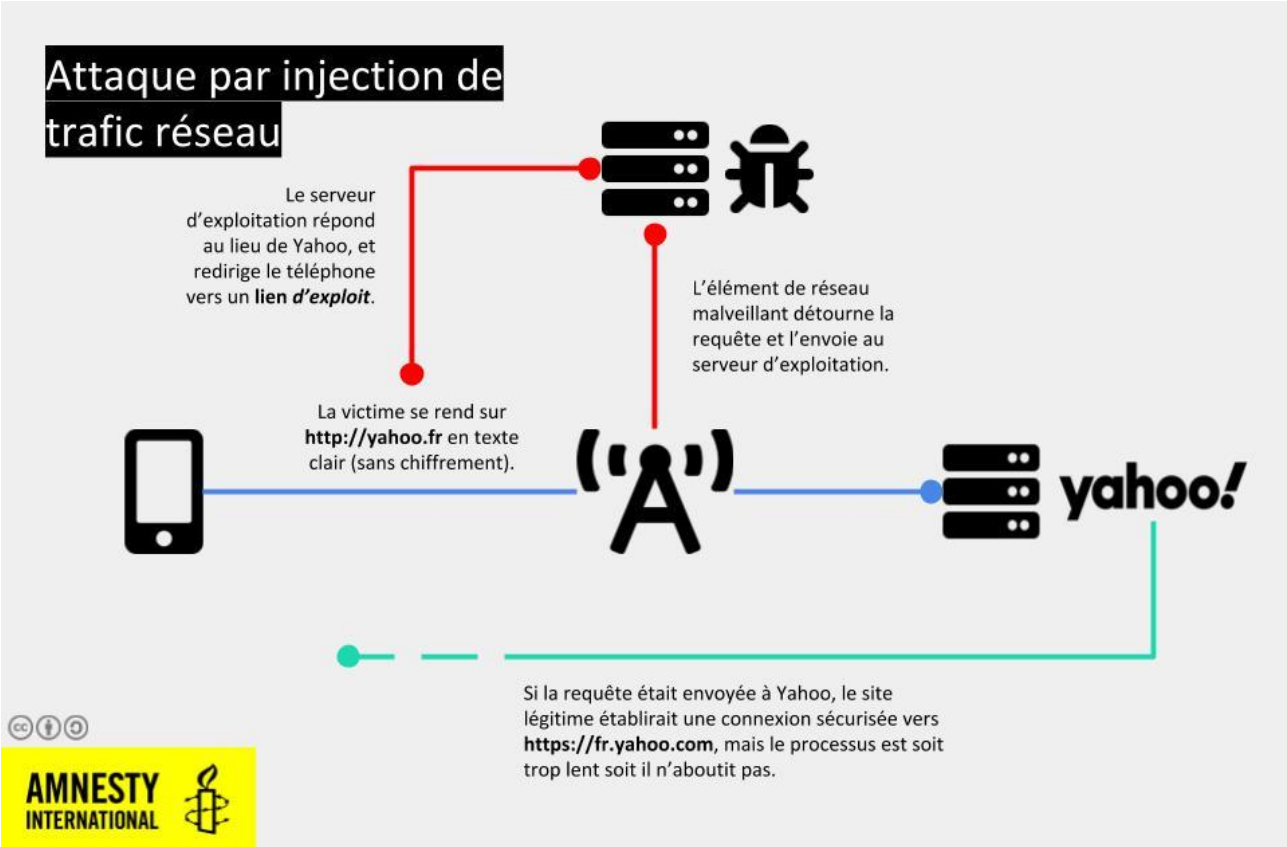
Après une trentaine de secondes, Maati Monjib a réessayé d'accéder à Yahoo, en tapant cette fois « *yahoo.fr mail* » sur Google, et a fini par être dirigé vers le bon site, où il a pu consulter son courrier électronique.

Nous pensons que ces redirections sont le signe d'une attaque par injection de trafic réseau généralement appelée attaque de l'homme du milieu (MITM). Cette méthode permet à un attaquant ayant un accès privilégié à la connexion réseau d'une cible de surveiller et de détourner le trafic, tel que les requêtes web, selon son bon vouloir. L'attaquant peut ainsi changer le comportement de l'appareil ciblé, comme dans ce cas, pour le rediriger vers des téléchargements malveillants ou des pages de l'*exploit* sans qu'aucune autre interaction de la victime ne soit nécessaire.

Cette position avantagée au niveau du réseau peut être n'importe quel élément du réseau aussi proche que possible de l'appareil ciblé. Dans le cas présent, l'appareil ciblé étant un iPhone, qui ne se connecte que sur une ligne mobile, une position avantagée pourrait être une tour cellulaire malveillante placée non loin de la cible ou une autre infrastructure de cœur de réseau dont l'opérateur mobile peut avoir reçu une demande de reconfiguration pour permettre ce genre d'attaques.

Cette attaque étant exécutée de manière invisible en passant par le réseau plutôt qu'en ayant recours à des SMS malveillants et à la fraude psychologique, elle a l'avantage de ne nécessiter aucune interaction de l'utilisateur et de ne laisser aucune trace visible par la victime.

Nous pensons que c'est ce qui s'est passé avec le téléphone de Maati Monjib. Alors qu'il consultait yahoo.fr, son téléphone était surveillé et détourné et Safari était directement dirigé vers un serveur d'exploitation qui a ensuite tenté d'installer silencieusement un logiciel espion.



En poussant plus loin notre analyse de l'appareil, nous avons identifié au moins quatre tentatives similaires d'injection entre mars et juillet 2019. (Remarque : à chaque tentative, l'URL redirigée changeait légèrement et présentait des sous-domaines, un numéro de port et une URI différents.)

Nous pensons qu'au moins une attaque par injection a réussi et compromis l'iPhone de Maati Monjib. Un autre détail découvert sur le téléphone conforte nos soupçons.

Lorsqu'une application plante, iPhone conserve dans un fichier journal la trace des causes précises du plantage. Ces journaux de crash sont stockés sur le téléphone pour une durée indéfinie, au moins jusqu'à ce que le téléphone soit *synchronisé* avec iTunes. On peut les trouver dans *Réglages > Confidentialité > Analyse > Données d'analyse.* Notre examen du téléphone de Maati Monjib a montré qu'à une occasion tous ces fichiers de crash ont été effacés quelques secondes après l'une de ces redirections de Safari. Nous pensons qu'il s'agissait d'un nettoyage délibéré exécuté par le logiciel espion pour effacer les traces pouvant conduire à l'identification des vulnérabilités activement exploitées. Ce nettoyage a été suivi par l'exécution d'un

processus suspect et par une réinitialisation forcée du téléphone.

Nous ne disposons pas actuellement d'informations suffisantes pour attribuer de façon certaine ces attaques présumées par injection de trafic réseau aux produits ou services de NSO Group. Ceci étant dit, certaines similitudes techniques avec d'autres infections attribuées à Pegasus, ajoutées au fait que Maati Monjib ait déjà été ciblé par le logiciel de NSO et que NSO fasse la promotion des capacités d'injection de trafic réseau qui, d'après nos suspicions, auraient été utilisées dans cette attaque nous permettent de penser que des outils de NSO peuvent aussi avoir été utilisés dans cette attaque.

Nous avons confirmé que Maati Monjib avait déjà été pris pour cible par le logiciel espion Pegasus de NSO Group au moyen de SMS malveillants. Les liens figurant dans ces messages ressemblent fortement aux URL utilisées dans les attaques par injection de trafic réseau :

Exemple de lien d'injection de trafic réseau	Exemple de lien figurant dans les SMS de Pegasus
`hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz`	`hxxps://videosdownload[.]co/nBBJBIP`

Ces deux liens sont composés de noms de domaine relativement génériques suivis d'une chaîne aléatoire de 7 à 9 caractères.

En outre, une capacité d'injection de trafic réseau similaire est brièvement décrite dans le document intitulé "Pegasus – Product Description" – vraisemblablement rédigé par NSO – découvert lors d'une fuite de données en 2015 du concurrent italien Hacking Team, qui commercialisait lui aussi des logiciels espions.

> **Installation de proximité (distance limitée) :**
>
> ▪ **Élément de réseau tactique :** L'agent Pegasus peut être injecté silencieusement après obtention du numéro grâce à un élément de réseau tactique tel qu'une station de transmission de base (BTS). Pegasus profite des capacités de ces outils tactiques pour réaliser une injection et une installation à distance de l'agent. Prendre position dans le secteur de la cible suffit, dans la plupart des cas, pour effectuer l'acquisition du numéro de téléphone. Une fois le numéro obtenu, l'installation se fait à distance.

Dans ce document, NSO Group désigne la position avantagée comme un « élément de réseau tactique » (Tactical Network Element) et explique comment une tour cellulaire malveillante (ou station de transmission de base) peut être utilisée pour identifier le téléphone de la cible, puis y injecter et installer Pegasus à distance.

Pourquoi est-ce condamnable ?

Lorsque des personnes sont visées par une activité de surveillance fondée sur le seul

exercice de leurs droits humains, cela équivaut à une atteinte « arbitraire ou illégale » à leur vie privée et bafoue leur liberté d'expression énoncée dans le Pacte international relatif aux droits civils et politiques. Cibler Maati Monjib et Abdessadak El Bouchattaoui pour le simple fait de travailler en faveur des droits humains est contraire aux principes définis par le droit international relatif aux droits humains.

Ce n'est pas la première fois que le logiciel espion manufacturé par NSO Group est utilisé contre des défenseur·e·s des droits humains. Ce logiciel a non seulement été utilisé pour cibler une personne membre du personnel d'Amnesty International en 2018, mais aussi pour attaquer des personnes qui défendaient les droits humains en Arabie saoudite, au Mexique et aux Émirats arabes unis.

NSO Group affirme que cette technologie n'est utilisée qu'à des fins licites, contre des terroristes et des criminels, par exemple, et que si les États utilisent ses outils à mauvais escient, ses mécanismes de diligence requise en matière de droits humains sont suffisants pour enquêter sur ces utilisations inappropriées et en assurer la réparation. Plus tôt ce mois-ci, NSO Group a par ailleurs publié sa politique en matière de droits humains. En l'absence de transparence suffisante en ce qui concerne les mécanismes de diligence requise et les enquêtes de NSO sur les utilisations inappropriées, Amnesty International juge depuis longtemps ces affirmations fallacieuses. Les révélations détaillées dans ce rapport montrent avec une évidence accrue que les affirmations de NSO Group et sa politique en matière de droits humains ne sont qu'une tentative visant à blanchir les atteintes aux droits causées par l'utilisation de ses produits.

En vertu des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, NSO Group et son principal investisseur, la société de capital-investissement britannique Novalpina Capital, doivent immédiatement prendre des mesures proactives pour s'assurer de ne pas causer d'atteintes aux droits humains ni d'y contribuer dans le cadre de leurs opérations internationales, et pour remédier à de telles atteintes lorsqu'elles se produisent. Pour s'acquitter de cette responsabilité, NSO Group est tenu d'appliquer une politique de diligence requise relative aux droits humains, et de prendre des mesures pour veiller à ce que les personnes qui défendent les droits humains au Maroc ne soient plus la cible d'une surveillance illégale.

Amnesty International a écrit à NSO Group et Novalpina Capital pour connaître leur opinion sur les informations détaillées dans ce rapport. La réponse qu'a envoyée NSO Group se trouve en Annexe I. L'entreprise y affirme de nouveau que les allégations d'utilisation à mauvais escient vont faire l'objet d'une enquête. Amnesty International insiste auprès de NSO Group pour que ces investigations se déroulent de manière transparente et attends de voir quelles actions concrètes vont être menées pour répondre de manière satisfaisante aux sujets d'inquiétude soulevés dans le présent rapport.

Enfin, les autorités marocaines devraient révéler les détails de tout accord passé avec NSO Group et veiller à ce que les personnes qui défendent les droits humains soient protégées contre toute surveillance illégale au moyen de garanties juridiques et gouvernementales adaptées et conformes aux normes internationales, notamment en offrant des voies de recours efficaces aux personnes pour qu'elles puissent dénoncer les atteintes à leurs droits humains liées à la surveillance.

Si vous avez reçu des SMS semblables à ceux décrits dans ce rapport, vous pouvez nous les communiquer en écrivant à l'adresse suivante :

share@amnesty.tech

Annexe I – Réponse de NSO Group

« Conformément à notre politique, nous enquêtons sur les allégations d'utilisation frauduleuse de nos produits. Si une enquête identifie des conséquences dommageables réelles ou potentielles sur les droits humains, nous prenons rapidement et de manière proactive des mesures pour y remédier. Nous pouvons par exemple suspendre l'utilisation du produit par un client ou y mettre directement un terme, comme nous l'avons déjà fait par le passé.

Malgré les importantes contraintes juridiques et contractuelles concernant notre capacité à commenter si un organisme public en particulier a autorisé l'exploitation de nos produits, nous prenons ces allégations au sérieux et allons enquêter sur le sujet tel que le prévoit notre politique. Nos produits sont conçus pour aider les services de renseignement et d'application des lois à sauver des vies. Ils n'ont pas pour fonction de surveiller les dissidents ou les militants pour les droits humains. C'est pourquoi les contrats que nous passons avec tous nos clients n'autorisent l'utilisation de nos produits qu'à des fins légitimes de prévention du crime et du terrorisme et pour enquêter sur de tels actes. Si jamais nous découvrons que nos produits ont été utilisés de manière non conforme à ce contrat, nous prendrons les mesures appropriées. »

ANNEXE II – Messages SMS

Jour et heure	Cible	Message	Lien final
23-10-2017 18h00	Abdessadak El Bouchattaoui	Nouveau à temara La 1 ère fois à Bd Fouarate Apparts avec jardin,grandes piscines & Salle sport + 2 piscines chauffées 7/7 6000/m2. Pour ne plus recevois nos	hxxp://stopsms[.]biz/TY8us0h

		SMS : hxxp://stopsms[.]biz/TY8us0h	
02-11-2017 12h29:33	Maati Monjib	TruecalIer à le plaisir de vous annoncer l'ajout d'une nouvelle fonctionnalité, consulter les noms des personnes qui ont cherché votre numéro durant une semaine hxxp://tinyurl[.]com/y73qr7mb	hxxps://revolution-news[.]co/ikXFZ34ca
02-11-2017 16h42:34	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 16h44:00	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 16h45:10	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 16h57:00	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 17h13:45	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 17h21:57	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 17h30:49	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
02-11-2017 17h40:46	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
15-11-2017 17h05:17	Maati Monjib	فضيحة أخلاقية داخل مقهى بورتز في حي أكدال بالرباط لمشاهدة الفيديو الذي يوثق \r\n الفضيحة hxxps://videosdownload[.]co/nBBJBIP	hxxps://videosdownload[.]co/nBBJBIP
20-11-2017 18h22:03	Maati Monjib	فاجعة الصويرة تسقط أول المسؤولين أمام القضاء hxxps://infospress[.]com/LQoHgMCEE	hxxps://infospress[.]com/LqoHgMCEE
23-11-2017 15h37:14	Maati Monjib	Bonjour,Quelqu'un vous a recherché sur Truecaller.Découvrez de qui il s'agit. hxxp://tinyurl[.]com/y93yg2sc	hxxps://business-today[.]info/k8mc8FJpz
24-11-2017 13h43:17	Maati Monjib	Nhar lekbir c'est le vendredi 24	hxxps://hmizat[.]co/JaCTkfEp

		Novembre ! Soyez au Rendez-vous sur notre site : hxxp://tinyurl[.]com/y9hbdqm5 \nvous pouvez consulter nos offres du moment	
24-11-2017 17h26:09	Maati Monjib	Vous l'avez demandé, CityClub l'a fait!Grand retour du BLACKFRIDAY vendredi 24/11!\r\nRéservez votre carte promo 15 mois à 1633dh! 0522647000 STOPSMS: hxxps://stopsms[.]biz/2Kj2ik6	hxxps://stopsms[.]biz/2Kj2ik6
27-11-2017 15h56:10	Maati Monjib	Le BackFriday continue exceptionnellement aujourd'hui chez CityClub! Dernière chance de s'offrir 15MOIS de fitness à 1633!\r\nDemain il sera trop tard 0522647000 STOPSMS: hxxps://stopsms[.]biz/yTnWt1Ct	hxxps://stopsms[.]biz/yTnWt1Ct
07-12-2017 18h21:57	Maati Monjib	ALQODS RESTERA TOUJOURS LA CAPITALE DE LA PALESTINE SAUVEZ LA VILLE SAINTE EN SIGNANT CETTE PETITION hxxp://tinyurl[.]com/y7wdcd8z	hxxps://infospress[.]com/Ln3HYK4C
08-01-2018 12h58	Maati Monjib	Urgent le livre sur Donald Trump s est arrache dans toutes les librairies une version arabe est disponible gratuitement sur le	hxxps://infospress[.]com/asjmXqiS

		lien hxxp://tinyurl[.]com/y87hnl3o	