NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Pegasus , le logiciel de guerre israelien

Pegasus est un logiciel espion destiné à attaquer les smartphones sous iOS et Android. Il est conçu et commercialisé dès 2013 par l'entreprise israélienne NSO Group et les premières traces de ses intrusions ne sont découvertes qu'en 2016.

Installé à distance sur un appareil, il peut contourner tous les systèmes de sécurité et accéder aux fichiers, messages, photos et mots de passe sur les smartphones. Il peut aussi **écouter les appels téléphoniques, et déclencher l'enregistrement audio, la caméra ou la géolocalisation.**

Pegasus est considéré comme une arme de guerre.

Sa vente nécessite une licence d'exportation du Ministère Israélien de la Défense. Pour des raisons de sécurité nationale, Israël ne permet pas qu'il cible les pays de l'alliance « Five Eyes », qui regroupe Etats-Unis, le Canada, le Royaume-Uni, l'Australie et la Nouvelle-Zélande1.

En juillet 2021, le Projet Pegasus, une enquête journalistique collaborative internationale, révèle que le logiciel a été utilisé par plusieurs pays à des fins d'espionnage. Parmi les cibles identifiées, on dénombre 189 journalistes, 85 militants des droits de l'homme, 65 dirigeants d'entreprises et 600 personnalités politiques ou membres de gouvernements et des chefs d'états2,3.

Éditeur, commercialisation et découverte

de son existence

La société israélienne NSO Group fabrique et commercialise des équipements de pointe destinés à lutter contre le terrorisme et le crime organisé[4] et le logiciel Pegasus fait partie de son offre. L'acquisition d'une licence peut atteindre 25 000 $ par cible[5], mais varie en fonction du nombre de cibles. En 2016, le New York Times expliquait ainsi que les clients de NSO devait d'abord s'acquitter d'une facture de **500 000 $ de frais d'installation, puis d'un forfait de 650 000 $ pour 10 iPhone ou 10 Android. Cent cibles supplémentaires étaient facturés 800 000 $, cinquante 500 000 $, vingt 250 000 $, dix 150 000 $[6]. Chaque vente doit être validée par le ministère israélien de la Défense**[7].

Le groupe NSO fait face à plusieurs poursuites reliées à l'utilisation du logiciel espion[7]. Une fuite de courriels indique que le logiciel est commercialisé dès août 2013, date à laquelle les Émirats arabes unis l'achètent[8]. En 2016, grâce à la vigilance de l'opposant émirati Ahmed Mansoor exilé au Canada, les chercheurs du Citizen Lab de l'université de Toronto découvrent Pegasus sur son téléphone[9].

Caractéristiques techniques

Le logiciel Pegasus utilise les failles de sécurité des systèmes d'exploitation des smartphones (iOS ou Android). S**on fonctionnement technique évolue ainsi en permanence[10].**

Vulnérabilités

Les vulnérabilités zero-day étant très difficiles à trouver — elles font l'objet d'un véritable marché dans lequel des hackers vendent leurs trouvailles au plus offrant[11] —, elles ont un coût élevé[12], par exemple, jusqu'à 2,5 millions d'euros pour une faille concernant le système d'exploitation Android[13]. La découverte de vulnérabilités sur iOS est relativement rare, mais Pegasus exploite de nouvelles vulnérabilités au fur et à mesure qu'elles sont détectées et avant qu'elles ne soient corrigées par Apple[12,14].

Par exemple, dès 2016, l'iPhone 6 a été la cible de Pegasus qui exploitait plusieurs vulnérabilités logées dans la bibliothèque WebKit. Les failles

permettent, en chargeant une page web, d'exécuter du code tiers sur l'iPhone puis de réaliser un Jailbreak d'iOS sur un iPhone ; ensuite, le logiciel chargé localise les zones mémoire du noyau de système d'exploitation pour les modifier, mettant hors d'usage les différentes couches de protection applicative. Le piratage se termine par le téléchargement et l'installation de Pegasus15.

Installation

L'installation du logiciel sur le smartphone visé peut se faire par plusieurs moyens16 :

- par spear phishing : elle nécessite que l'utilisateur clique sur un lien envoyé via un sms ou un iMessage qui exploite ensuite des failles logicielles10,16,2 ;
- par redirection internet : l'utilisateur est redirigé à son insu vers une autre URL que celle du site web qu'il souhaite visiter17 ;
- par radiocommunication : depuis mai 2018, NSO recourt à des techniques dites « *zero click* » qui installent Pegasus sans action de l'utilisateur17. Ces techniques s'appuient notamment sur les vulnérabilités zero-day de divers logiciels17, comme Whatsapp, iMessage ou Apple Music13 ;
- par émetteur-récepteur sans fil à proximité du terminal ;
- manuellement : si le smartphone de la cible est dans les mains du commanditaire16.

Données récupérées

Pegasus fournit au commanditaire un large accès aux données du téléphone, incluant les sms et les messages (y compris chiffrés) envoyés et reçus, le carnet d'adresses, il peut activer micro et caméra, capter les données de localisation GPS et permettre l'enregistrement des appels téléphoniques16,18. Il peut accéder aussi aux publications sur les réseaux sociaux, aux photos, aux vidéos, aux enregistrements. Il a accès aux historiques des consultations internet. Il peut aussi retracer l'itinéraire de son utilisateur19. Par exemple, Pegasus est capable de capter des données d'applications, comme WhatsApp, Skype, Facebook ou Gmail. Il peut aussi enregistrer tous les caractères saisis sur le téléphone ou photographier l'écran20.

Furtivité

Le logiciel espion Pegasus est sophistiqué et modulaire, en plus de permettre une personnalisation selon le pays d'utilisation ou les propriétés achetées par l'utilisateur final. Il utilise un chiffrement pour se protéger de la détection des outils de sécurité traditionnels et dispose d'un mécanisme de surveillance et d'autodestruction21. Les versions les plus récentes du logiciel sont susceptibles de se loger uniquement dans la mémoire vive du smartphone, et non sa mémoire permanente, ce qui permet d'en faire disparaître toute trace lors de l'extinction du téléphone16. Enfin, lorsque des ONG ou journalistes publient des éléments sur le fonctionnement du logiciel, NSO Group l'adapte pour qu'il demeure furtif10.

Architecture

L'architecture technique du système s'appuie sur trois niveaux : une station de travail, un serveur informatique d'infection et une infrastructure cloud. L'opérateur lance son attaque depuis sa station, ce qui provoque l'envoi du SMS piégé. Le lien qu'il incorpore pointe vers l'un des serveurs web de l'infrastructure cloud. Le serveur web redirige la victime ensuite vers le serveur d'infection qui va exécuter l'attaque15.

Utilisation du cloud

Pegasus s'appuie sur les serveurs informatiques d'Amazon Web Services (AWS), filiale d'Amazon et de serveurs hébergés en Europe, dont ceux d'OVH22. À la suite des révélations du Projet Pegasus en juillet 2021, Amazon débranche ces serveurs. Selon le laboratoire de recherches canadien Citizen Lab, les services informatiques d'AWS constituent un pilier important de l'infrastructure technique de Pegasus, sans pour autant constituer le cœur de son infrastructure informatique23.

Détection

Pour vérifier si un téléphone intelligent est infecte une analyse technique par des experts en sécurité informatique est nécessaire. Dans le cadre de l'enquête journalistique du projet Pegasus, le Security Lab d'Amnesty International, qui par ailleurs offre pour les initiés un outil de détection, a analysé des téléphones ciblés et y a détecté des traces d'intrusions. La méthode de détection a été validée de

manière indépendante par les chercheurs du Citizen Lab de l'université de Toronto[24,25]. La société Suisse DigiDNA annonce une application de détection des traces de Pegasus[26].

États clients

L'entreprise NSO Group qui revendique une quarantaine de clients étatiques[10] travaille en relation avec le gouvernement israélien qui délivre les autorisations d'exportation[27]. Parmi les États qui utiliseraient le logiciel **figurent, l'Allemagne, l'Espagne, l'Arabie saoudite, l'Azerbaïdjan, Bahreïn, les Émirats arabes unis, la Hongrie, l'Inde, le Kazakhstan, le Maroc, le Mexique, le Panama, la Pologne, le Rwanda le Ghana, le Togo, et le Salvador[28,29,30,31,1,32,33,34]. En septembre 2022, au total, vingt-six pays sont client de NSO group pour l'utilisation de ce logiciel[33].**

Approchés par NSO dès 2019, **les services de renseignement français sont intéressés par Pegasus. La décision de ne pas l'acheter est prise en haut lieu fin 2020**[35].

A rebours de ce qui était affirmé sur la non utilisation en Israël, le quotidien "Calcalist" soutient que la police israélienne a utilisé, depuis 2013, le logiciel Pegasus de manière intensive, sans supervision judiciaire et de façon illégale[36].

Selon le New York Times, le FBI a acheté en 2019 une licence d'une version dédiée de Pegasus pour le tester, sans donner suite au projet après les révélations journalistiques du « Projet Pegasus » en 2021. L'entreprise NSO a développé une version du logiciel pour ses éventuels clients américains baptisée « Phantom » permettant de cibler les téléphones américains[37].

Utilisations abusives contre des opposants politiques et journalistes

L'utilisation du logiciel est controversée et si l'entreprise revendique une utilisation légale de cette technologie (enquêtes criminelles comme celle qui a mené à l'arrestation du baron de la drogue El Chapo), Pegasus est dans la pratique utilisé par des agences de renseignements étatiques, parfois de dictatures, pour espionner des journalistes, des opposants politiques et des

militants des droits de l'homme[38].

Dès 2015

L'Espagne utilise Pegasus contre le mouvement indépendantiste catalan dès 2015[39]. Selon Citizen Lab, l'activiste politique catalan et professeur universitaire Jordi Sànchez aurait été le premier indépendantiste visé en 2015 à la suite d'une manifestation à Barcelone, bien que la majorité des cas d'espionnage contre le mouvement indépendantiste catalan se sont produits entre 2017 et 2020[40].

Enquête de 2016

Les premières révélations sortent en 2016 sur la société israélienne NSO Group[41]. Le 25 août 2016, le laboratoire Citizen Lab et l'entreprise Lookout (en) révèlent que le smartphone du militant des droits de l'homme Ahmed Mansoor a été ciblé par un logiciel espion nommé Pegasus[42]. Ahmed Mansoor est un militant émirati, lauréat 2015 du prix Martin Ennals. Le 10 août 2016, il informe les chercheurs du Citizen Lab, Bill Marczak et John Scott-Railton, qu'il vient de recevoir deux SMS suspects sur son iPhone 6. Ces SMS promettent de lui révéler des secrets sur les prisonniers torturés dans les prisons des Émirats arabes unis (EAU). Mansoor devient immédiatement suspicieux : il a été emprisonné pour son activisme et est régulièrement la cible de malwares commerciaux que les analystes ont rattachés au gouvernement des EAU[42],[43].

L'analyse publiée par Citizen Lab et Lookout indique que l'URL du SMS (qui relève de l'hameçonnage ciblé) dirige vers le téléchargement d'un logiciel malveillant qui exploite trois vulnérabilités critiques dites « zero-day » du système d'exploitation iOS, dénommé Trident. Le logiciel s'installe alors discrètement sur l'iPhone sans en informer l'utilisateur et transmet au commanditaire de nombreuses données (localisation GPS, communications, photos, liste des contacts, accès aux micro et caméra, etc.)[21],[44],[19],[45]. Les chercheurs découvrent que le virus est un produit référencé par NSO Group, appelé Pegasus dans des documents confidentiels[21]. Des détails du logiciel espion confirment aux chercheurs que son emploi n'est pas nouveau et remonte à plusieurs années[46].

Enquêtes postérieures

Au Mexique, le gouvernement d'Enrique Peña Nieto qui a payé **80 millions de dollar**s sa copie du logiciel, a suivi le journaliste mexicain Javier Valdez Cárdenas, assassiné en 2017, et au moins huit autres journalistes, des opposants politiques et des enquêteurs internationaux comme le démontre le Citizen Lab de l'université de Toronto[47],[48].

En Arabie saoudite, il a servi contre des activistes, notamment un confident de Jamal Khashoggi en octobre 2018[49].

En mai 2019, le Citizen Lab a alerté Facebook, propriétaire de WhatsApp, après avoir découvert une activité suspecte dans le téléphone d'un avocat britannique, Yahya Assiri (en), impliqué dans des poursuites visant NSO Group. L'entreprise est accusée de fournir à l'Arabie saoudite des outils pour pirater les téléphones d'Omar Abdulaziz (vlogger) (en), un dissident saoudien installé au Canada — dont l'espionnage est susceptible d'avoir concouru à l'assassinat de Jamal Khashoggi —, un citoyen qatarien et un groupe de journalistes et de militants mexicains[50],[51],[52],[53]. Dès le 12 mai, WhatsApp reconnait publiquement qu'une vulnérabilité de son logiciel[54] permet au groupe NSO d'infecter un téléphone par un simple appel, même laissé sans réponse, et il invite toute sa base d'usagers à installer une mise à jour[55]. *In fine*, WhatsApp évalue à 1 400 le nombre d'utilisateurs dont les téléphones ont été infectés par Pegasus[56].

L'ONG Citizen Lab établit qu'en 2019 le téléphone de Roger Torrent, président du Parlement de Catalogne, a été ciblé par ce logiciel espion[57].

En mai 2019, Amnesty International a déposé un affidavit en Israël demandant de cesser la vente et la distribution du logiciel espion parce que celui-ci menace le droit à la vie privée et à la liberté d'opinion et d'expression, en violation des obligations d'Israël[58],[59].

En août 2020, le journal *Le Monde* révèle, d'après une enquête menée conjointement avec le journal *The Guardian*, que six Togolais, opposants au régime en place ou dignitaires religieux, dont M^{gr} Benoît Alowonou, évêque du diocèse de Kpalimé, ont été la cible d'espionnage via l'utilisation du logiciel Pegasus[60].

Quelques mois plus tard, en décembre 2020, le laboratoire Citizen Lab révèle que plus d'une trentaine de journalistes de la chaîne de télévision qatarie Al Jazeera ont été pris pour cible par Pegasus, probablement à l'initiative de l'Arabie saoudite et des Émirats arabes unis[61],[62].

Le 16 juillet 2020, Pablo Iglesias, le secrétaire général du parti Podemos et membre du gouvernement espagnol réclame l'ouverture d'une enquête parlementaire sur la surveillance par logiciel ayant visé plusieurs militants du mouvement indépendantiste catalan. Le Guardian et El Pais avaient révélé qu'au moins trois indépendantistes catalans, dont le président du Parlement de Catalogne, avaient été visés en 2019 par Pegasus[63].

Enquête de Forbidden Stories en juillet 2021

Article détaillé : Projet Pegasus (journalisme).

En juillet 2021, une enquête nommée « Projet Pegasus » du collectif de journalistes Forbidden Stories s'appuyant sur l'expertise technique d'Amnesty International (Security Lab d'Amnesty International), montre que le logiciel est utilisé à des fins politiques par onze États, notamment pour espionner des opposants, des militants, des journalistes et des juges[64],[65].

Parmi les mille cibles potentielles identifiées, sur 50 000 numéros de téléphone présélectionnés par des États, on dénombre 189 journalistes, 85 militants des droits de l'homme, 65 dirigeants d'entreprises et 600 personnalités politiques ou membres d'instances gouvernementales, dont plusieurs chefs d'État[2],[3].

Révélations ultérieures

En 2021, le rapport *Citizen Lab*[66] a révélé que le gouvernement bahreïnien utilise Pegasus pour suivre au moins neuf militants depuis le 20 juin. Entre juin 2020 et février 2021, neuf militants ont été ciblés pour être membres de l'une de ces organisations politiques d'opposition, une ONG des droits de l'homme ou des dissidents exilés. De plus, certains militants ont été piratés par une entité nommée « LULU », quelques uns ont été piratés en utilisant deux exploits d'iMessage à zéro clic[67].

En septembre 2021, les médias belges *Knack* et *Le Soir* indiquent que, selon les autorités belges, des journalistes belges ont été espionnés via le logiciel Pegasus.

Le service de renseignement militaire (SGRS) considère qu'il est « très probable » qu'ils l'aient été par le Rwanda68.

En octobre 2021, Cheikh Mohammed ben Rached al-Maktoum utilise Pegasus pour pirater les téléphones de la princesse Haya Bint Al Hussein et de ses avocats dans une affaire de divorce à Londres69.

En novembre 2021, une analyse menée par le Security Lab d'Amnesty International révèle qu'un militant de l'autodétermination du Sahara occidental est espionné en Belgique. Mahjoub Mleiha est la quatrième victime du logiciel espion Pegasus sur le sol belge. Il a vu son téléphone infecté à plusieurs reprises début 202170.

En décembre 2021, une enquête du Projet Pegasus a révélé que le téléphone de Kamel Jendoubi, président du Groupe d'experts des Nations Unies sur la guerre au Yémen, a été infecté par le logiciel espion Pegasus par l'Arabie saoudite en 201971. Amnesty International confirme aussi que des opposants kazakhs ont été pris pour cible, après analyse de leurs téléphones72.

En janvier 2022, Front Line Defenders constate que le téléphone d'Ebtisam al-Saegh, une défenseur des droits de l'homme au Bahreïn, a été piraté au moins huit fois entre août et novembre 2019. Celui de Hala ahed Deeb, qui travaille avec les droits de l'homme et les groupes féministes en Jordanie, l'a été en mars 202173,74.

En février 2022, l'analyse légale par Amnesty International75 et Citizen Lab76 a montré que les téléphones de trois militants à Bahreïn étaient ciblés par Pegasus entre juin et septembre 2021. Premièrement, un avocat, Mohamed Al-Tajer, a défendu des activistes et combattu pour des réformes démocratiques. Son téléphone a été infecté par le logiciel Pegasus en septembre 2021, juste après que soit dévoilé qu'il était espionné par un logiciel concurrrent77. Deuxièmement, la psychiatre Sharifa Siwar a accusé l'un des fils du roi d'être compromis dans un trafic de médicaments. Son téléphone a été infecté en juin 2021. Troisièmement, un journaliste en ligne, qui a demandé l'anonymat, a couvert notamment le soulèvement de Bahreïn en 2011 et possède de nombreux contact parmi les activistes. Son téléphone a été infecté en septembre 202178.

En avril 2022, Citizen Lab a publié un rapport40 confirmant qu'au moins 63 individus, membres du Parlement européen en faveur de l'indépendance de la

Catalogne, présidents catalans, juristes représentant des catalans éminents et membres d'organisations catalanes telles que l'Assemblé nationale catalane et Òmnium Cultural ont été visés par Pegasus, notamment entre 2017 et 2020. Le 5 mai 2022, la responsable des services secrets espagnols, Centro Nacional de Inteligencia (CNI), Paz Esteban, a admis que des indépendantistes catalans avaient été espionnés via Pegasus, mais assure que cette surveillance a été menée dans un cadre légal79.

Le rapport Citizen Lab a publié que les deux bureaux de Boris Johnson, 10 Downing Street et Bureau des Affaires étrangères et du Commonwealth, ont été ciblés à plusieurs fois à l'aide de Pegasus par les Émirats arabes unis en 2020 et 202180.

Le 2 mai 2022, il est confirmé que le téléphone du premier ministre espagnol a été infecté au printemps 2021 par le logiciel Pegasus81.

En 2023, une enquête de l'Union européenne établit que le logiciel a été utilisé contre des membres de l'opposition d'États membres de l'union, notamment en Pologne et en Hongrie82.

Utilisation par la police en Israël

En Israël, l'utilisation de Pegasus par la police israélienne pose question. En 2022, elle est accusée d'espionnage à grande échelle sans autorisation particulière de personnalités, de proches du gouvernement, de journalistes ou d'hommes d'affaires. De manière générale, les demandes à la justice de mise sur écoutes de personnes spécifiques ne précisent pas les outils utilisés83,84. Toutefois des « conclusions intermédiaires » d'une enquête du ministère de la Justice israélien évoquent « des informations incorrectes et certainement inexactes »85.

Utilisation contre le commissaire européen à la justice

En avril 2022, Didier Reynders, commissaire européen à la Justice révèle à l'agence de presse Reuters avoir été ciblé par le logiciel Pegasus. Trois autres membres de la commission auraient également été visés, et les commanditaires du piratage restent inconnus86,87.

Poursuites judiciaires

Article détaillé : NSO Group#Poursuites judiciaires.

A la suite des révélations du Projet Pegasus, plusieurs personnes morales – dont Amnesty International, Apple et WhatsApp, filiale de Meta portent plainte contre NSO Group, éditeur du logiciel espion Pegasus88,89,90.

Article détaillé : Projet Pegasus (journalisme)#Réactions et conséquences.

Plusieurs personnes physiques effectivement espionnées ou sélectionnées pour un espionnage potentiel déposent ou annoncent déposer plainte.

L'affaire a entraîné de multiples enquêtes judiciaires et parlementaires, et des sanctions internationales91,34.

Notes et références

1. ↑ Revenir plus haut en :a et b Damien Leloup et Martin Untersinger, *« Pegasus : le service de renseignement extérieur allemand a également utilisé le logiciel espion »* [archive], sur LeMonde.fr, 8 octobre 2021 (consulté le 29 janvier 2022).
2. ↑ Revenir plus haut en :a b et c (en) Dana Priest, Craig Timberg et Souad Mekhennet, « *Private Israeli spyware used to hack cellphones of journalists, activists worldwide* », *The Washington Post*, 18 juillet 2021 (lire en ligne [archive]).
3. ↑ Revenir plus haut en :a et b *« À propos du Projet Pegasus »* [archive], sur Forbidden Stories.org, 18 juillet 2021.
4. ↑ Cellule investigation de Radio France, *« Le Projet Pegasus en cinq questions »* [archive], sur FranceInter.fr, 20 juillet 2021 (consulté le 20 juillet 2021).
5. ↑ *« Technical Analysis of Pegasus Spyware : An Investigation Into Highly Sophisticated Espionage Software »* [archive], sur info.lookout.com, Lookout, 2016.
6. ↑ *« How Spy Tech Firms Let Governments See Everything on a Smartphone »* [archive], sur nytimes.com, 2016

7. ↑ Revenir plus haut en :a et b (en) John Scott-Railton et Ronald J. Deibert, « *Governments are deploying spyware on killers, drug lords and journalists* », *The Globe and Mail*, 3 mai 2019 (lire en ligne [archive]).
8. ↑ (en) David D. Kirkpatrick et Azam Ahmed, « *Hacking a Prince, an Emir and a Journalist to Impress a Client* », *The New York Times*, 31 août 2018 (lire en ligne [archive]).
9. ↑ (en) *« Government Hackers Caught Using Unprecedented iPhone Spy Tool »* [archive], sur vice.com (consulté le 27 juillet 2021).
10. ↑ Revenir plus haut en :a b c et d Florian Reynaud, « *« Projet Pegasus » : dans les coulisses de la traque d'un logiciel espion sophistiqué* », *Le Monde*, 18 juillet 2021 (lire en ligne [archive]).
11. ↑ Florian Reynaud, « *Vendus comme très sûrs, les iPhone ont été piratés par Pegasus pendant des années* », *Le Monde*, 20 juillet 2021 (lire en ligne [archive]).
12. ↑ Revenir plus haut en :a et b *« Failles Trident sur iOs et Spyware Pegasus : tout comprendre sur cette attaque qui a fait trembler Apple »* [archive], sur Advens, 31 août 2016 (consulté le 7 décembre 2018).
13. ↑ Revenir plus haut en :a et b *« Pegasus : que sait-on du logiciel qui a servi à espionner des militants, journalistes et opposants du monde entier ? »* [archive], sur SudOuest.fr, 19 juillet 2021 (consulté le 20 juillet 2021).
14. ↑ *« Apple répare une faille informatique liée au logiciel d'espionnage Pegasus »* [archive], sur LeMonde.fr avec AFP, 14 septembre 2021 (consulté le 14 septembre 2021).
15. ↑ Revenir plus haut en :a et b Gilbert Kallenborn, *« Comment fonctionne Pegasus, ce malware qui vole toutes les données de l'iPhone »* [archive], sur 01net.com, 26 août 2016 (consulté le 21 juillet 2021).
16. ↑ Revenir plus haut en :a b c d et e (en) David Pegg et Sam Cutler, « *What is Pegasus spyware and how does it hack phones?* », *The Guardian*, 18 juillet 2021 (lire en ligne [archive]).
17. ↑ Revenir plus haut en :a b et c (en) *« Forensic Methodology Report: How to catch NSO Group's Pegasus »* [archive], Amnesty International, 18 juillet 2021.
18. ↑ (de) « *Mächtige Spionage-Software für iPhones entdeckt* », *Der Standard*, 26 août 2016 (lire en ligne [archive], consulté le 1er septembre 2016).
19. ↑ Revenir plus haut en :a et b *« Le projet Pegasus révèle les faiblesses des*

iPhone » [archive], sur France Culture, 20 juillet 2021 (consulté le 20 juillet 2021).

20. ↑ Martin Untersinger, *« Découverte d'une version pour Android du logiciel espion Pegasus »* [archive], sur LeMonde.fr, 5 avril 2017 (consulté le 20 juillet 2021).
21. ↑ Revenir plus haut en : a b et c *« Technical Analysis of Pegasus Spyware : An Investigation Into Highly Sophisticated Espionage Software »* [archive], sur info.lookout.com, Lookout, 2016.
22. ↑ *« Comment fonctionne le logiciel espion Pegasus ? »* [archive], sur Le Monde Informatique, 21 juillet 2021.
23. ↑ *« « Projet Pegasus » : Amazon débranche les serveurs de l'entreprise de surveillance NSO Group »* [archive], sur LeMonde.fr, 19 juillet 2021 (consulté le 20 juillet 2021).
24. ↑ Nicolas Six, *« « Projet Pegasus » : comment savoir si l'on a été infecté par le logiciel de surveillance ? »* [archive], sur LeMonde.fr, 20 juillet 2021 (consulté le 23 juillet 2021).
25. ↑ *« Comment les données du « Projet Pegasus » ont été analysées »* [archive], sur LeMonde.fr, 18 juillet 2021 (consulté le 23 juillet 2021).
26. ↑ (en) *« Detect Pegasus malware on iOS for free using admin app iMazing »* [archive], sur AppleInsider (consulté le 4 août 2021).
27. ↑ *« «Projet Pegasus». Qu'est-ce que NSO group, la société qui a vendu le logiciel espion dans 40 pays ? »* [archive], sur Ouest France, 19 juillet 2021.
28. ↑ (en) Phineas Rueckert, *« Pegasus: The new global weapon for silencing journalists »* [archive], Forbidden Stories, 18 juillet 2021.
29. ↑ (en) David D. Kirkpatrick et Azam Ahmed, « *Hacking a Prince, an Emir and a Journalist to Impress a Client* », *The New York Times*, 31 août 2018 (lire en ligne [archive]).
30. ↑ Fabrice Arfi, Camille Polloni et Ilyes Ramdani, *« « Projet Pegasus » : des révélations d'une ampleur mondiale sur la surveillance »* [archive], Mediapart, 19 juillet 2021.
31. ↑ *« Pegasus : la police fédérale allemande était également cliente du logiciel* .....

sources : B.F. , wikipedia license CC