CRSI
CENTRE DE RÉFLEXION
SUR LA SÉCURITÉ INTÉRIEURE

NOTE FLASH
Novembre 2021

## Démocratisation des cyberarmes
## Montée en puissance des cyber-menaces

# Une analyse de l'Affaire Pegasus

**Marc-Olivier BOISSET** Analyste associé au CRSI
**Jean LANGLOIS-BERTHELOT** Analyste associé au CRSI

Le 18 juillet 2021, le consortium international de journalistes « Forbidden Stories » publiait une enquête intitulée « *The Pegasus Project* »[1]. C'est un coup de tonnerre : selon l'enquête, le logiciel espion Pegasus, commercialisé par l'entreprise israélienne NSO Group, est utilisé depuis plusieurs années pour surveiller de façon systématique des journalistes, des activistes et d'autres membres de la société civile. Le 13 septembre, Apple diffusait une mise à jour de sécurité d'iOS, son système d'exploitation pour l'IPhone. Il s'agissait pour Apple d'apporter une réponse technique au scandale, ses téléphones ayant démontré leur vulnérabilité face à Pegasus.

Mais deux semaines après les premières révélations, déjà, différents éléments techniques recueillis par les autorités françaises dans le cadre de l'enquête judiciaire tendaient à confirmer le travail réalisé par ce consortium de dix-sept médias[2]. Ainsi, par exemple, en analysant le téléphone d'un journaliste de la chaîne de télévision France 24, l'Agence nationale de sécurité des systèmes d'information (ANSSI), chargée de la cybersécurité de l'État, a confirmé la présence de traces du passage de Pegasus.

Les données techniques récupérées sur le téléphone par l'agence de cybersécurité ont confirmé que l'appareil du journaliste avait à minima subi une phase d'étude approfondie en vue d'une cyberattaque : des adresses de courriers électroniques de comptes Apple en lien avec une infrastructure d'attaque liée à NSO Group étaient présentes sur le mobile du correspondant de France 24. Les mêmes identifiants ont été récupérés chez d'autres cibles de NSO Group : Omar Radi, journaliste marocain actuellement en prison, Claude Mangin, épouse d'un militant du Sahara occidental également incarcéré au Maroc, mais aussi François de Rugy, un des ministres français qui auraient été visés par Pegasus.

NSO Group n'en est pas à son coup d'essai. Elle avait déjà fait l'objet de révélations cinq ans auparavant, le 25 août 2016, par le laboratoire Citizen Lab et l'entreprise Lookout. Ces-derniers avaient démontré à l'époque que le téléphone portable du militant émirati des droits de l'homme Ahmed Mansoor avait été la cible du même logiciel espion. Le militant avait reçu deux SMS suspects, qui promettaient de lui faire des révélations sur les tortures de prisonniers aux seins des prisons émiriennes. Suite aux investigations techniques, il s'avère que le lien contenu dans les SMS reçus entrainait le téléchargement d'un logiciel malveillant, nommé Trident. Celui-ci exploite trois vulnérabilités dites « *zero day* »[3] du système d'exploitation d'Apple. Une fois le téléphone portable de la cible infecté par ce logiciel, celui-ci diffuse vers le commanditaire l'historique des localisations GPS, les communications, les photographies, la liste des contacts, le son capté par le micro et la vidéo prise par la caméra, et ce à l'insu de l'utilisateur. Ces incidents sont caractéristiques d'une véritable démocratisation de l'accès aux cyberarmes par les organisations publiques, mais aussi privées.

## La démocratisation des cyberarmes

En 1998, le film « Ennemi d'État », de Tony Scott, véritable thriller technologique d'anticipation, mettait en scène l'avocat Robert Clayton Dean (Will Smith) poursuivi par la puissante National Security Agency (NSA)[4], qui emploie toutes ses capacités techniques pour essayer de l'éliminer. Cette fiction mettait en exergue toutes les possibilités offertes par le cyberespace pour collecter des informations voir entraver une cible.

Pendant longtemps, les capacités techniques utilisées nécessitaient des investissements importants : en 2013 le budget de la NSA s'élevait à 10,8 milliards de dollars[5] sur un budget total consacré aux rensei-

[1] Forbidden Stories, 2021
[2] « Le Monde», 2021
[3] Ces vulnérabilités n'ont pas fait l'objet d'une mise à jour de sécurité par l'éditeur du logiciel et peuvent ainsi être exploitées par un attaquant, par exemple pour extraire des données personnelles à l'insu de l'utilisateur.
[4] La NSA est la principale agence de renseignement technique américaine chargée des écoutes mondiales et de la surveillance électronique.
[5] « Le Monde », 2013

gnements par les Américains de 66,7 milliards de dollars[6]. Peu d'États étaient en mesure de consentir un tel effort financier pour se doter de capacités de cyberattaque performantes. Vingt ans après « Ennemi d'État », avec l'expansion du cyberespace, force est de constater que le paradigme a changé et que les cyberarmes, en particulier les capacités de cybersurveillance, ne sont plus l'apanage des organisations publiques disposant d'une expertise technique de haut niveau. Les acteurs ne disposant pas des compétences techniques pour concevoir ce type d'outils peuvent désormais les acquérir facilement auprès d'organisations privées comme NSO Group. « *C'est un marché en plein essor. Il y a multiplication des acteurs et des méthodes d'espionnage proposées* », selon Bastien Bobe, expert de l'entreprise Lookout[7]. On assiste ainsi depuis une dizaine d'années à une véritable démocratisation de l'arme cyber dont l'Affaire Pegasus ne constitue que la partie émergée de l'iceberg.

## *« L'Affaire Pegasus constitue la partie visible de cette guerre invisible qui a lieu dans le cyberespace »*

Le principal risque de cette démocratisation des cyberarmes est la banalisation de l'usage de ces capacités techniques par les acteurs publics, mais surtout à terme privés. En effet, « *on constate souvent que les armes cyber utilisés par les États se retrouvent in fine en vente sur le marché noir de la cybercriminalité* », rappelle Philippe Rondel de Check Point Software Technologies France[8]. La vie privée des individus sera ainsi davantage exposée à des actes de cybercriminalité. Cette banalisation des outils a d'ailleurs déjà augmenté le nombre d'acte de cybercriminalité. À ce titre, l'Internet Crime Report du FBI[9] souligne que 241 342 attaques par phishing ont été signalés en 2020, contre 114 702 en 2019, soit une augmentation de 50 % de ce type d'attaque. Cet accroissement des actions de phishing risque d'entrainer à court terme une augmentation des actions de chantage numérique[10].

De plus, avec l'avènement de la technologie 5G, cette démocratisation devrait s'accélérer. En effet, le déploiement de cette nouvelle norme de télécommunication va provoquer une forte augmentation du volume d'objets connectés: les spécialistes estiment à environ 30 milliards le nombre de ces objets aujourd'hui et ils s'attendent à un accroissement de plus de 20 % par an[11]. Le risque est que ces objets soient détournés de leur usage initial pour collecter des informations sur un individu à son insu. À titre d'exemple, Alexis Viguié et Adrien Albisetti ont découvert que le robot connecté Monsieur Cuisine connect, commercialisé par l'enseigne Lidl, dispose d'un microphone fonctionnel qui n'apparait dans aucune fiche technique de l'appareil[12]. Ils ont réussi à faire fonctionner ce micro et ont pu discuter à distance, via une application de messagerie vocal. Lidl a expliqué que ce micro était présent « au cas où » le produit serait amélioré avec un assistant vocal afin d'être commandé par la voix. Cet accroissement de la surface numérique des organisations et des individus, basé sur des objets connectés plus ou moins sécurisés, va de facto multiplier les opportunités de cyberattaques pour les organisations publiques et privées. Le niveau de cybersécurité des systèmes numériques, ainsi que les capacités techniques de cyberprotection, constitueront des éléments encore plus déterminants pour l'efficacité d'une stratégie de cyberdéfense.

### La cybersécurité, enjeu majeur pour les organisations

L'Affaire Pegasus constitue la partie visible de cette guerre invisible qui a lieu dans le cyberespace depuis plusieurs années déjà. La diversification des acteurs en mesure d'utiliser ces capacités risque d'augmenter le brouillard de guerre, complexifiant encore davantage l'attribution des cyberattaques. L'utilisation d'acteurs privés dans cet espace permet aux États de brouiller les pistes et d'échapper plus facilement à une potentielle attribution de leurs actions : l'entreprise privée devient une véritable « société écran numérique », elle constitue une garantie supplémentaire d'anonymat pour l'État à l'origine des attaques dans le cyberespace. On devrait ainsi assister à une intensification des tensions dans le cyberespace entre les différents acteurs publics, mais aussi privés : les groupes terroristes, en particulier devraient profiter de cet accès à de nouvelles capacités techniques et augmenter le volume de leurs actions de cyberterrorisme.

Cette multiplication des acteurs aura également un effet sur la ressource humaine : elle augmentera à court terme la pression sur le recrutement de talents dans le domaine de la cybersécurité, qui constitue aujourd'hui une difficulté majeure pour les États. Cette ressource demeure aujourd'hui largement insuffisante pour répondre à l'ensemble des besoins publics et privés. En France, les entreprises de cybersécurité éprouvent de grandes difficultés à recruter et à garder leur ressource humaine[13].

Pour faire face à l'augmentation des cyberattaques, il semble primordial pour les États de conti-

[6] Office of the Director of National Intelligence, 2021
[7] France 24, 2021
[8] Ibid
[9] FBI, 2020
[10] Le cybercriminel exige de sa victime de l'argent en échange de secrets inavouables qu'il aura pu récupérer en s'introduisant dans ses systèmes numériques.
[11] Press, 2016
[12] Capital, 2019
[13] Meddah, 2020

nuer à agir à minima selon trois axes. En premier lieu, il est essentiel de poursuivre la sensibilisation du grand public sur l'importance de l'hygiène informatique. En effet, la majorité des incidents ou des attaques réussissent grâce à des erreurs humaines. Réduire ces erreurs permet de limiter les chances de succès des cyberattaques. Dans ce domaine, une bonne hygiène numérique peut par exemple facilement permettre de contrecarrer une attaque par phishing

Ensuite, il est nécessaire de poursuivre le développement de capacités de cyberdéfense. Cet effort de développement doit s'effectuer dans deux domaines. D'une part, il est utile pour protéger son organisation de disposer de systèmes dédiés de cyberprotection, par exemple pour la détection des attaques complexes. D'autre part, il demeure nécessaire d'améliorer le niveau minimal de cybersécurité de tous les systèmes numériques. À ce titre, un renforcement des normes de sécurité informatique apparait comme une piste intéressante à étudier pour protéger les libertés fondamentales des individus. L'exemple du robot commercialisé par Lidl souligne à quel point il est essentiel pour les fabricants d'objets connectés d'améliorer le niveau de sécurité de leurs objets.

*« La course aux capacités de cyberdéfense ne fait que commencer... et ne cessera pas »*

Enfin, la mise en place de partenariats entre États semble aussi indispensable, tant cette menace demeure diffuse et non-territorialisé. Réussir à attribuer une cyberattaque constitue un enjeu de taille pour les États, tant le cyberespace offre d'opportunités de masquer sa véritable identité, voire d'usurper celle d'un autre.

La course aux capacités de cyberdéfense ne fait que commencer et ne cessera pas, tant la numérisation de nos sociétés devrait se poursuivre à un rythme effréné. Face à cette numérisation à outrance, il conviendra de s'attacher lors du développement de nouveaux systèmes de respecter le concept de « frugalité numérique » (i.e. s'interroger sur la nécessité de numériser certaines fonctions) pour limiter les opportunités d'attaque cyber. ■

**Bibliographie**

*Capital. (2019, 06 13). Les vices cachés du Monsieur Cuisine connect de Lidl. Consulté sur Capital: https://www.capital.fr/entreprises-marches/les-vices-caches-du-monsieur-cuisine-connect-de-lidl-1341819*

*FBI. (2020). Internet Crime Report 2020. FBI.*

*Forbidden Stories. (2021, 07 18). The Pegasus project. Récupéré sur Forbidden Stories: https://forbiddenstories.org/case/the-pegasus-project/*

*France 24. (2021, 07 20). Pegasus, l'arbre qui cache la forêt du marché de la cybersurveillance étatique. Récupéré sur France 24: https://www.france24.com/fr/%C3%A9co-tech/20210720-pegasus-l-arbre-qui-cache-la-for%C3%AAt-du-march%C3%A9-de-la-cybersurveillance-%C3%A9tatique*

*Le Monde. (2013, 08 29). Espionnage : le «budget noir» américain rendu public. Récupéré sur Le Monde: https://www.lemonde.fr/ameriques/article/2013/08/29/espionnage-le-budget-noir-des-etats-unis-rendu-public_3468693_3222.html*

*Le Monde. (2021, 07 29). « Projet Pegasus » : les analyses des autorités françaises confirment l'infection des téléphones personnels de plusieurs journalistes. Récupéré sur Le monde: https://www.lemonde.fr/projet-pegasus/article/2021/07/29/projet-pegasus-les-analyses-des-autorites-francaises-confirment-l-infection-de-telephones-de-journalistes_6089946_6088648.html*

*Meddah, H. (2020, janvier 15). Cybersécurité recherche experts désespérément. Récupéré sur L'usine nouvelle: https://www.usinenouvelle.com/article/cybersecurite-recherche-experts-desesperement.N919064*

*OFFICE of the DIRECTOR of NATIONAL INTELLIGENCE. (2021). U.S. Intelligence Community Budget. Récupéré sur OFFICE of the DIRECTOR of NATIONAL INTELLIGENCE: https://www.dni.gov/index.php/what-we-do/ic-budget*

*Press, G. (2016, Septembre 2). Internet Of Things By The Numbers: What New Surveys Found. Récupéré sur Forbes: https://www.forbes.com/sites/gilpress/2016/09/02/internet-of-things-by-the-numbers-what-new-surveys-found/#2b50369016a0*

*Zone militaire. (2018, 10 31). En 2018, le budget du renseignement américain s'est élevé à 81,5 milliards de dollars, en hausse de 11,6%. Récupéré sur Opex360: http://www.opex360.com/*