RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 26 novembre 2025
Nombre de pages : 43

TÉLÉPHONES MOBILES

ÉTAT DE LA MENACE DEPUIS 2015

TLP:CLEAR

Table des matières

SYNTHÈSE

L'omniprésence, l'usage systématique des *smartphones* et la multiplication des fonctionnalités et données qu'ils traitent en font des cibles d'intérêt pour l'acquisition de renseignements d'origine cyber.

Ces équipements du quotidien présentent des vulnérabilités et une surface d'attaque importante au niveau des différentes couches du terminal. Ces vulnérabilités se situent au niveau des interfaces sans fil, des applications, du système d'exploitation du téléphone mobile, voire dans des composants matériels.

D'une part, les différents protocoles de communication employés, tels que les réseaux mobiles, le Wi-Fi, le Bluetooth ou le NFC, présentent de nombreuses faiblesses permettant d'intercepter les informations échangées, voire d'en altérer les données afin de déployer des logiciels espions sur les terminaux.

D'autre part, le système d'exploitation et les applications installées sur le terminal peuvent également constituer des vecteurs d'intrusion pour le déploiement de logiciels espions. Certaines menaces sophistiquées exploitent en effet des chaînes de vulnérabilités jour-zéro qui ne nécessitent aucune interaction des cibles pour les infecter, communément nommées zéro-clic. Les implants mis en œuvre après l'obtention d'un accès au terminal mobile sont généralement non persistants et ne laissent donc que peu de traces sur les équipements compromis. La sophistication des chaînes d'infection et leur furtivité, ainsi que l'absence de solutions de détection, compliquent significativement les investigations numériques.

Cette surface d'attaque présente ainsi de multiples opportunités d'attaques dont cherchent à se saisir plusieurs acteurs offensifs disposant parfois de capacités très avancées.

Le ciblage de téléphones mobiles à des fins d'espionnage ou de surveillance peut être effectué par des acteurs étatiques ayant développé ces capacités en interne ou au travers de leur base industrielle et technologique de défense nationale. Mais ces capacités sont également commercialisées par des entreprises privées, spécialisées dans la lutte informatique offensive privée (LIOP).

Certaines entreprises de LIOP facilitent ainsi l'accès à ces capacités avancées pour des États ne disposant pas de ces technologies en propre ou souhaitant compliquer le processus d'attribution [1]. Ce faisant, elles participent à la multiplication des sources de menaces et la dissémination incontrôlée de ces outils, augmentant le niveau de menace associé.

En novembre 2023, lors du Forum de Paris sur la Paix [2], la France et le Royaume-Uni ont lancé des consultations pour lutter contre la prolifération et l'usage irresponsable des outils offensifs commerciaux. Cette initiative, appelée Processus de Pall Mall depuis son lancement formel à Londres en février 2024, a mené à l'élaboration d'une doctrine de bonne conduite à destination des États [1]. Pour lutter contre ces menaces, elle encourage à la fois à une meilleure coopération des constructeurs pour renforcer la sécurité des équipements mobiles mais également à augmenter le partage d'informations sur les menaces observées, tout en recommandant des cadres règlementaires relatifs à l'utilisation et la vente de telles capacités.

1. Si l'imputation lie une activité malveillante à un mode opératoire sur la base d'éléments techniques et contextuels, l'attribution associe une attaque à un commanditaire dans un objectif politique ou géopolitique.

2. Évènement annuel regroupant des chefs d'État et de gouvernement, des représentants d'organisations internationales et de la société civile ayant pour objectif de servir d'espace de coopération pour favoriser la réflexion sur les modalités d'actions collectives pour répondre aux enjeux globaux.

L'ANSSI a traité au cours des trois dernières années de multiples compromissions de téléphones issues de l'utilisation irresponsable [3] de logiciels espions à l'encontre d'individus ayant des fonctions au sein de hautes autorités gouvernementales ou de comités de direction d'entreprises de secteurs stratégiques. Dans la majorité des cas, l'ANSSI a observé un ciblage des téléphones personnels des victimes.

En outre, les téléphones mobiles sont des cibles de choix pour les cybercriminels. Pour mener ces attaques à finalité lucrative, ils emploient des codes malveillants peu avancés et des techniques d'ingénierie sociale afin de collecter des données personnelles ou professionnelles des victimes. Ces données, en fonction de leur nature, peuvent être réutilisées pour mener des campagnes d'hameçonnage ou accéder à des systèmes d'information. Le ciblage opportuniste des cybercriminels affecte les particuliers et les entités sans distinction de secteurs ou de zones géographiques.

> **i**
>
> **Que faire en cas de notification de menace par un éditeur**
>
> En cas de réception de signalements (courriels, SMS...) issus des éditeurs de solutions et avertissant d'une potentielle compromission d'un compte ou d'un appareil, il est fortement conseillé de ne pas manipuler votre téléphone et de **contacter le CERT-FR** par courriel à l'adresse **cert-fr@ssi.gouv.fr** ou par téléphone au **3218** (service gratuit + prix d'un appel) ou +33 (0) 9 70 83 32 18.

3. Le Code de bonnes pratiques à destination des États du Processus de Pall Mall définit un « usage irresponsable » comme menaçant la sécurité, le respect des droits de l'Homme et des libertés fondamentales ou la stabilité du cyberespace, ou sans garanties ni mécanismes de supervision adéquats, ou d'une manière qui soit incompatible avec le droit international applicable ou avec le cadre consensuel des Nations Unies sur le comportement responsable des États dans le cyberespace.

1 AVANT-PROPOS

Cet état de la menace sur les équipements mobiles se concentre sur la menace pesant sur les téléphones mobiles intelligents ou ordiphones grand public.

Il s'appuie sur des incidents traités par l'ANSSI, des rapports d'organismes officiels, d'éditeurs de sécurité, d'organisation non gouvernementales, ainsi que des informations pertinentes issues de sources ouvertes afin de dresser une vue d'ensemble de l'état des connaissances sur ce type de menace.

Cet état de la menace présente d'abord les vecteurs et modalités techniques d'exploitation employés pour compromettre les équipements mobiles puis les capacités et finalités des différents acteurs offensifs. Les éléments présentés dans cet état de la menace ne sont pas exhaustifs et ont été sélectionnés pour illustrer les différentes opportunités, capacités et finalités du ciblage de téléphones mobiles. Des recommandations, proposées au fil de l'eau, sont développées à la fin du rapport. Les recommandations de sécurité (présentées dans la partie 4 du document) permettent de réduire la surface d'attaque de ces équipements. Elles s'adressent autant à l'utilisateur, qui est invité à lire attentivement ces recommandations s'il s'identifie dans l'une des cases présentées ci-dessous, qu'au responsable de la sécurité des systèmes d'information (RSSI).

Suis-je une cible de logiciel espion ?

Le ciblage au moyen de logiciels espions sophistiqués peut concerner des individus traitant de sujets sensibles ou en lien avec les intérêts fondamentaux de la Nation, afin de collecter de l'information pouvant être de valeur pour un État étranger. Par exemple, des membres de hautes autorités de la fonction publique, des élus, des comités de direction d'entreprises stratégiques, des avocats, des journalistes, des militants ou activistes, des dissidents ou des proches de personnes précédemment mentionnées peuvent faire l'objet d'un ciblage.

À l'inverse, l'ensemble de la population peut être victime de vols d'identifiants ou de compromission de son téléphone mobile par des cybercriminels.

2 OPPORTUNITÉS LIÉES AUX ÉQUIPEMENTS MOBILES : VECTEURS TECHNIQUES ET MODALITÉS D'EXPLOITATION

2.1 Surface d'attaque associée aux interfaces sans fil

Les interfaces mobiles sont des dispositifs ou des protocoles permettant la communication entre deux éléments, par exemple entre une antenne-relais et un téléphone mobile. Ces communications par ondes radio permettent d'échanger des données sans contact physique. Comme pour tout protocole réseau, des identifiants uniques sont attribués à chaque équipement mobile permettant de les distinguer les uns des autres. Ces protocoles de communication, qu'il s'agisse de la 2G, 3G, 4G et 5G, du Wi-Fi, du Bluetooth ou du NFC, présentent des faiblesses exploitables par des acteurs malveillants.

Les attaques ciblant les interfaces sans fil ont trois principaux objectifs :

- **Interception passive** : interception des données, c'est-à-dire des identifiants de l'équipement mobile et des données brutes échangées, par un positionnement à proximité d'une communication ;
- **Interception active** [4] : déchiffrement, détournement de la communication grâce à un positionnement de l'attaquant entre les deux équipements, par exemple par l'emploi d'une technique de *Adversary-in-the-middle* (AITM), et captation des informations ;
- **Altération des données** : interception active, détournement et modification des communications à des fins de compromission du terminal mobile.

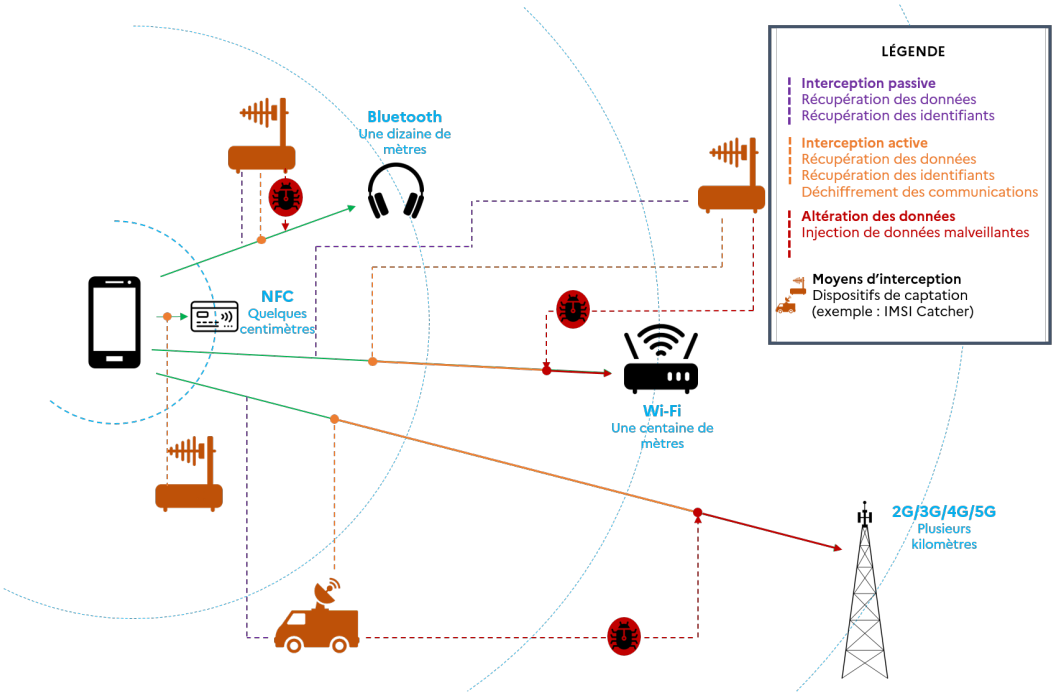

FIGURE 1 – Attaques ciblant différentes interfaces mobiles

4. Ce type d'interception émet des signaux radio et est ainsi détectable.

2.1.1 Exploitation du protocole 2G

Le protocole 2G est une technologie de communication spécifique aux téléphones mobiles [5] dont les principaux usages sont les communications vocales, les messages *via* le protocole SMS et l'accès à Internet [6].

Si les messages SMS sont échangés sans chiffrement au préalable, la confidentialité des communications vocales en 2G est assurée par un algorithme [7] de chiffrement faible et cassé publiquement en 2010. Ce protocole, contrairement aux protocoles 3G ou 4G, ne dispose d'aucun mécanisme d'authentification des antennes-relais auprès des terminaux [2]. Il n'est donc pas possible pour un équipement mobile de vérifier la légitimité d'une antenne-relais avant de s'y connecter, permettant ainsi les attaques de type AITM.

Le réseau 2G a été progressivement remplacé par des normes de téléphonie mobile plus sécurisées [8] et est déjà décommissionné dans plusieurs pays du monde comme les États-Unis ou le Japon [9]. Il reste cependant encore utilisable afin de garantir une couverture réseau dans des zones non connectées aux protocoles 3G, 4G ou 5G.

Ces faiblesses et cette rétrocompatibilité offrent une capacité d'interception à proximité notamment exploitée dans les équipements de type *IMSI catcher* [10]. Ces derniers imitent les antennes-relais des opérateurs mobiles pour déconnecter la cible de son réseau opérateur et la reconnecter au réseau interne attaquant, captant ainsi l'ensemble des communications vocales, des messages et la géolocalisation de sa victime.

Ce type d'équipement est désormais présent dans les milieux criminels à travers des marchés de contrebande et des plateformes commerciales étrangères. Certains attaquants s'en servent ainsi pour collecter des numéros de téléphone et envoyer des SMS d'hameçonnage de manière massive dans des secteurs géographiques précis. Selon Libération, en 2022 à Paris, une voiture a été arrêtée avec un *IMSI catcher* activé dans son coffre dans le but d'envoyer des faux SMS liés à l'Assurance Maladie [3].

2.1.2 Exploitation des faiblesses du protocole Wi-Fi

Le Wi-Fi est un ensemble de protocoles sans fil connectant plusieurs appareils à proximité au sein d'un même réseau. Ces réseaux, et plus spécifiquement les réseaux Wi-Fi publics non sécurisés, peuvent présenter des vulnérabilités ou des faiblesses de configuration et être vulnérables à des attaques du type AITM : un acteur malveillant peut se positionner entre l'utilisateur et le point d'accès Wi-Fi pour intercepter, modifier et récupérer des informations sensibles. Si l'exploitation de réseaux Wi-Fi n'est pas spécifique aux équipements mobiles, plusieurs cas ont été publiquement documentés ces dernières années :

- **Exploitation de vulnérabilités ou de faiblesses de configuration** [11] : des entreprises de LIOP vendent des solutions conçues pour compromettre des périphériques Wi-Fi et cap-

5. Introduite dans les années 1990, elle permet l'échange de données numériques plutôt qu'analogiques.
6. Ce dernier a été intégré plus tardivement *via* la norme GPRS.
7. L'algorithme de chiffrement standardisé pour la 2G est le A5/1
8. Les normes de téléphonie mobile sont usuellement connues sous les noms 2G, 3G, 4G et 5G.
9. Le réseau 2G est destiné à être décommissionné en France en 2026.
10. Un *IMSI catcher*, ou intercepteur d'IMSI, est un appareil conçu pour collecter les identités (IMSI, IMEI) des téléphones mobiles 2G, 3G et 4G. Les *IMSI catcher* ne fonctionnent pas avec la 5G car le SUPI (*Subscription Permanent Identifier*), alternative à l'IMSI, est chiffré et non transmis durant l'établissement d'une connexion. Il est nécessaire d'utiliser un SUCI (*Subscription Concealed Identifier*) *catcher*, dont le numéro unique est généré à partir du SUPI.
11. Il existe plusieurs faiblesses de configuration Wi-Fi, comme l'utilisation de protocoles de sécurité obsolètes tels que le *Wired Equivalent Privacy* (WEP) ou encore l'absence de mot de passe pour se connecter au réseau.

ter *via* ce protocole l'ensemble des communications effectuées ainsi que la localisation de la victime en quasi temps réel. Un tel dispositif a été utilisé en 2022 pour rediriger le trafic des cibles vers chaînes d'exploitation du logiciel espion **Predator** [4, 5, 6].

- **Capacités d'interception Wi-Fi** : plusieurs entreprises de LIOP, comme la société israélienne MAGEN ou la société émirienne STRATIGN, développent et commercialisent des dispositifs d'interception Wi-Fi portatifs capables de capturer de manière massive les données transitant par ce protocole, sans laisser de traces [7].
- **Installation de faux points d'accès Wi-Fi** : ce type d'attaque cherche à tromper la vigilance de l'utilisateur en usant notamment de techniques d'ingénierie sociale pour l'inciter à se connecter à des réseaux ouverts opérés par des acteurs malveillants. Ces faux points d'accès Wi-Fi peuvent servir à collecter des identifiants en redirigeant les utilisateurs vers des pages d'hameçonnage ou à injecter du code malveillant sur les sites consultés afin de compromettre le téléphone [8, 9].

Recommandations sur l'utilisation du protocole Wi-Fi

- Désactiver la connexion Wi-Fi lorsqu'elle n'est pas utilisée.
- Désactiver la connexion automatique aux réseaux Wi-Fi connus ou ouverts.
- Ne pas se connecter à des points d'accès Wi-Fi publics sauf impératif et le cas échéant utiliser un VPN.

2.1.3 Exploitation du protocole Bluetooth

Le Bluetooth est une technologie de connexion sans fil permettant à des équipements électroniques de communiquer entre eux sur une distance limitée [12]. Comparativement au Wi-Fi, le Bluetooth est dédié à des échanges de faibles quantités de données. Cette technologie, utilisée pour l'échange de données avec des périphériques sans fil (casque audio, montre connectée, etc.), est également employée pour déverrouiller certaines voitures ou certaines portes de chambre d'hôtel.

Un téléphone dont l'interface Bluetooth est activée devient détectable. Ainsi, tout équipement radio dans un rayon d'une dizaine de mètres est en capacité de collecter son identifiant. En 2021, un chercheur norvégien a parcouru en 12 jours 300 kilomètres avec un dispositif artisanal de journalisation des interfaces Bluetooth et a observé le déplacement d'appareils d'utilisateurs dont le Bluetooth était activé [10]. Les technologies de pistage *via* Bluetooth sont commercialisées pour de la surveillance, mais également à des fins commerciales et marketing pour suivre les déplacements de clients dans des magasins, dans des lieux de loisirs ou dans les transports en commun [11, 12, 13, 14].

Les vulnérabilités liées à l'interface Bluetooth d'un équipement mobile peuvent être exploitées comme vecteur initial d'intrusion. Cette interface peut par exemple être exploitée en simulant la connexion d'un équipement pour injecter du code malveillant. Par ailleurs, des chaînes de vulnérabilités dont certaines ciblent l'interface Bluetooth peuvent conduire à une exécution de code à distance, comme **Blueborne** ciblant *Android* [15] ou **Airbone** ciblant *iOS* [16].

Le niveau de sécurité d'une connexion Bluetooth étant variable, il est également possible pour un acteur malveillant de déchiffrer les communications effectuées *via* cette technologie voire d'en altérer le contenu [17].

12. Selon la puissance, la technologie Bluetooth permet de connecter des appareils séparés d'une dizaine à une centaine de mètres.

Recommandations sur l'utilisation du protocole Bluetooth

- Désactiver l'interface Bluetooth lorsqu'elle n'est pas utilisée.
- Ne pas appairer l'équipement mobile à des dispositifs inconnus ou partagés.

2.1.4 Exploitation du protocole NFC

Le protocole NFC (*Near-Field Communication*) est un protocole de communication de proximité sans contact, limité à des échanges à faible distance, de quelques centimètres seulement. L'échange d'information s'effectue entre deux équipements : l'un est actif (téléphone, terminal de paiement), l'autre est actif ou passif (carte de paiement ou de transport). Les équipements passifs sont lisibles par n'importe quel équipement actif à proximité [13]. Aujourd'hui, la plupart des équipements mobiles comme les téléphones est compatible avec ce protocole.

L'usage du protocole NFC peut être détourné depuis un téléphone mobile. Selon ESET, en 2024, un groupe cybercriminel a lancé une campagne d'hameçonnage par SMS incitant les utilisateurs à cliquer sur un lien afin d'installer le code malveillant **NGate**. Ce code exploitait la capacité des téléphones à accéder à des informations *via* le protocole NFC. Une fois l'équipement mobile compromis, ce code permettait de lire les données de cartes de paiement à proximité pour les transmettre à l'attaquant afin d'effectuer des paiements [18].

Recommandation sur l'utilisation du protocole NFC

- Désactiver l'interface NFC sur le téléphone lorsqu'elle n'est pas utilisée.

2.1.5 Autres exploitations liées à l'opérateur de communication électronique

Certains vecteurs techniques ne sont pas directement liés aux équipements mobiles mais aux opérateurs de communications électroniques, dont les procédures organisationnelles peuvent également présenter des vulnérabilités à exploiter.

À titre d'exemple, la technique du *SIM-Swapping* [14] consiste à usurper l'identité de la victime auprès de son opérateur de télécommunications pour obtenir une nouvelle carte SIM sous le contrôle de l'attaquant. Celui-ci reçoit donc les communications SMS et les codes d'authentification à double facteurs (2FA) permettant la réinitialisation des mots de passe de la personne ciblée [19]. Les opérateurs du Mode Opératoire d'Attaque (MOA) cybercriminel Scattered Spider auraient intégré depuis 2022 le *SIM-Swapping* à leur arsenal d'attaque. En obtenant des informations personnelles de la victime, les cybercriminels peuvent usurper son identité auprès de l'opérateur et effectuer un échange de carte SIM. La récupération d'authentification multifacteurs peut ainsi leur permettre dans un second temps d'exfiltrer des données depuis un environnement bureautique en vue de le compromettre (déploiement d'un rançongiciel, vol de données, etc.) [5, 20].

13. En d'autres termes, il n'y a pas d'authentification mutuelle des équipements en NFC. Dans certains cas, comme le paiement par téléphone, l'authentification est effectuée directement par le téléphone mobile sans passer par le protocole NFC.
14. Le *SIM-Swapping* est une fraude par usurpation de carte SIM.

Commentaire : un renforcement des procédures des opérateurs de télécommunication relatives à la vérification des identités à distance des utilisateurs lors d'une demande de changement de carte SIM permettrait de réduire les attaques par SIM-Swapping [21].

Recommandation sur l'usage de l'authentification multifacteurs

- Activer le verrouillage par code PIN de la carte SIM.
- Changer le code PIN par défaut de la carte SIM.
- Privilégier l'usage d'applications d'authentication (*TOTP*) pour l'authentification multifacteurs.

2.2 Surface d'attaque associée au terminal

Si les premiers téléphones mobiles étaient dotés de systèmes d'exploitation très minimalistes, ils sont aujourd'hui comparables à des ordinateurs de bureau en termes de complexité et de fonctionnalités. Au delà de la partie matérielle d'un terminal principalement en charge des communications (voir partie 2.1), la partie logicielle est composée de deux couches principales : le système d'exploitation et les applications [15].

Le système d'exploitation installé par le constructeur gère le terminal, les composants physiques liés aux applications et les données de l'utilisateur. Ces différentes couches constituent une partie de la surface d'attaque d'un équipement mobile, et peuvent être ciblées au cours des différentes phases de la chaîne d'exploitation.

2.2.1 Vecteurs initiaux employés

Les vecteurs initiaux employés pour compromettre des téléphones mobiles peuvent émaner des interfaces réseau ou de l'exploitation du terminal. Trois principales méthodes, de niveaux de sophistication variés, sont observées pour le déploiement de code malveillant sur ce dernier :

- l'exploitation de vulnérabilité zéro-clic ;
- l'incitation à cliquer sur un lien ou un fichier malveillant ;
- l'installation grâce à un accès physique au terminal.

Dans certains cas, le recours au piégeage du matériel par le constructeur a été documenté. La compromission sur la chaîne d'approvisionnement reste à ce jour marginale.

Recommandations concernant la sécurisation du système d'exploitation

- Durcir le système d'exploitation en réduisant la surface d'attaque par la désactivation des fonctionnalités facultatives. Cela est possible sur *iOS* en activant le « *Mode Isolement* » ou sur *Android* en activant le « *Mode Protection Avancée* » depuis *Android* 16.
- Appliquer au plus vite les mises à jour du système d'exploitation et des applications installées sur le terminal.
- Ne pas reporter le redémarrage après la mise à jour de l'appareil.

Commentaire : l'ANSSI a pu constater, par ses propres moyens, l'efficacité du « Mode Isolement » pour bloquer des tentatives de compromissions.

15. Les applications sont les logiciels qui étendent les fonctionnalités du système d'exploitation et les usages du terminal. Elles peuvent être intégrées nativement au système d'exploitation ou ajoutées par l'utilisateur.

Exploitation au moyen de vulnérabilités zéro-clic

Les applications se synchronisant en permanence peuvent faire l'objet d'exploitation de vulnérabilités dites zéro-clic qui ne requièrent aucune action de la part de l'utilisateur. Parmi cette catégorie d'applications, les messageries instantanées comme *iMessage* ou *WhatsApp* sont régulièrement ciblées *via* ce type de vulnérabilités, du fait de leur présence très répandue sur les équipements mobiles. La vulnérabilité est alors exploitée de manière automatique lors du traitement des données, par exemple au moment de la réception et avant l'affichage du message ou de l'appel sur le téléphone. La compromission de ces applications constitue souvent la première étape de la chaîne d'exploitation dont l'objectif est d'exposer l'ensemble des données de l'appareil [16]. L'utilisation de plusieurs vulnérabilités sous forme de chaîne d'exploitation est un moyen nécessaire pour contourner chaque couche applicative afin de déployer un logiciel espion au plus près du coeur du système. La Figure 2 illustre le cheminement d'une telle chaîne d'exploitation, de la réception du message à la compromission du téléphone. L'exploitation de vulnérabilité zéro-clic en vecteur initial est très sophistiquée et a été documentée pour différentes chaînes d'exploitation associées à certains logiciels espions, telles que **Pegasus** depuis 2018 ou **Triangulation** depuis 2019 [22, 23, 24].

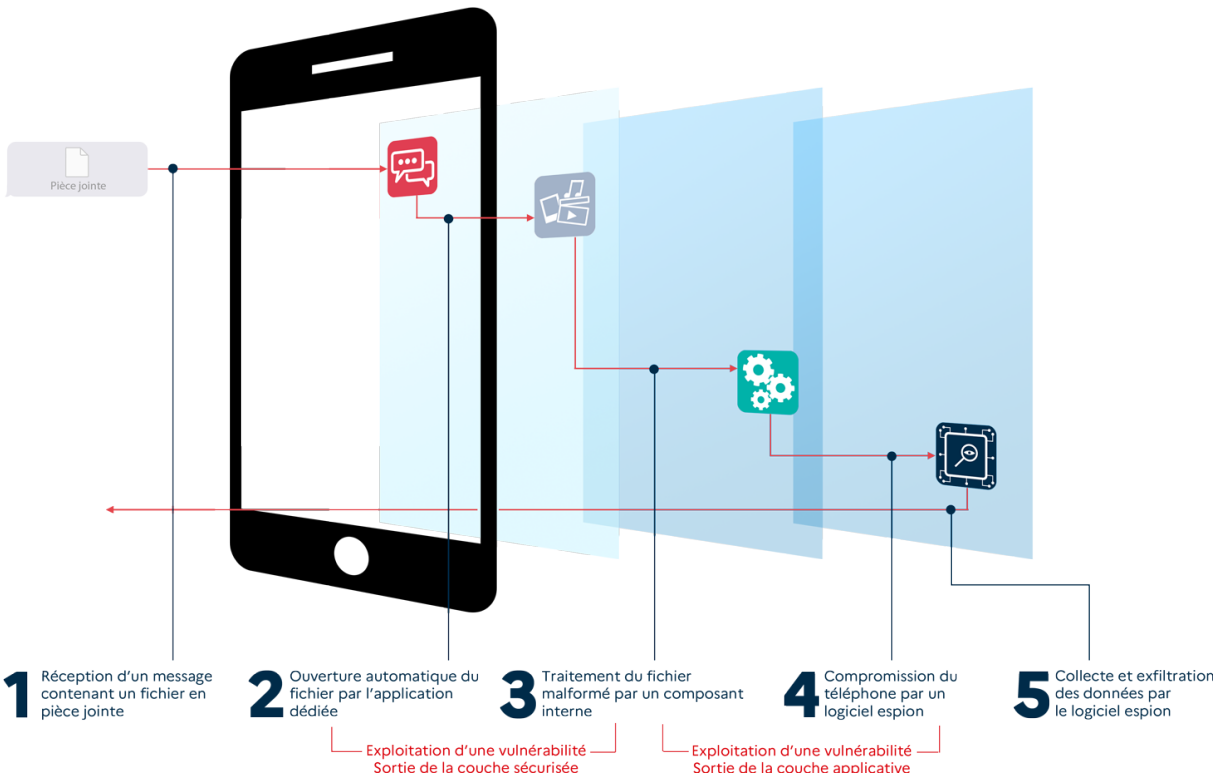

FIGURE 2 – Vue d'ensemble d'une chaîne d'exploitation zéro-clic

16. Une chaîne d'exploitation est une succession d'exploitation de vulnérabilités permettant à un attaquant de prendre progressivement le contrôle d'un système.

Recommandations concernant les applications de messagerie

- Désactiver les applications de messagerie pré-installées si elles ne sont pas utilisées.
- Désactiver la réception automatique des messages de type MMS.
- Éviter l'échange d'informations sensibles par SMS et préférer des messageries utilisant un chiffrement de bout en bout.
- Désactiver la sauvegarde automatique des conversations de ces applications.

Si les applications de messagerie sont les principales cibles de ces exploitations, d'autres applications natives telles que *Calendrier* sur *iOS* ont été utilisées comme vecteur de compromission zéro-clic dans une chaîne d'exploitation du logiciel espion **Reign**, documentée par CITIZEN LAB [25].

Les logiciels espions déployés grâce à des vulnérabilités zéro-clic sont les menaces les plus sophistiquées ciblant les équipements mobiles. Ces codes malveillants disposent notamment d'un niveau de furtivité élevé : ils peuvent dissimuler leurs communications entrantes et sortantes *via* des services légitimes, comme les versions récentes de **Pegasus** qui utilisent le service *iMessage* sur *iOS*, et se situent uniquement en mémoire pour ne laisser aucune trace [26]. Ces compromissions ne sont souvent pas persistantes [17]. L'attaquant est alors obligé de recompromettre sa victime à chaque redémarrage de l'équipement. Cette absence de persistance complexifie surtout la détection des logiciels espions et les investigations numériques des appareils infectés.

Commentaire : la complexité de la recherche des vulnérabilités zéro-clic amène certaines entreprises ou organes étatiques à employer d'autres vecteurs de compromission indétectables par l'utilisateur, tel qu'un accès au réseau par une coopération ou compromission de l'opérateur de téléphonie dont l'usage est défini dans la partie 3.1.1.1.

Recommandation concernant le redémarrage du téléphone

- Redémarrer régulièrement son téléphone.

Exploitation par ingénierie sociale

Les téléphones mobiles peuvent être compromis au moyen de techniques d'ingénierie sociale (*social engineering*) [18] incitant la victime à télécharger ou cliquer sur une ressource malveillante envoyée sur les réseaux sociaux, par SMS, par courriel ou *via* des messageries instantanées. Depuis au moins 2014, des campagnes d'hameçonnage associées à des modes opératoires (MOA) réputés liés à la Russie visant des utilisateurs de téléphones mobiles se sont ainsi appuyées sur la distribution de ressources malveillantes (fichiers ou liens) *via* des canaux légitimes tels que des forums, des courriels, des réseaux sociaux, ou encore des applications de messagerie comme *WhatsApp* ou *Signal* pour mener des campagnes à des fins d'espionnage [27, 28, 29, 30].

Des entreprises de LIOP développent également des réseaux de faux comptes sur les réseaux sociaux comme *Facebook* et *LinkedIn*. En 2024, l'entreprise META révélait avoir identifié puis démantelé des faux comptes liés à des entreprises de LIOP, utilisés à la fois pour tester leurs logiciels espions mais aussi à des fins de compromission *via* de l'ingénierie sociale. C'est le cas de l'entreprise espagnole MOLLITIAM SECURITY qui a mené une importante campagne

17. La persistance est une technique employée par les codes malveillants pour demeurer sur le système compromis, y compris après un redémarrage complet du terminal.
18. Technique exploitant la confiance ou la crédulité d'une personne afin de l'inciter à déclencher une action.

d'hameçonnage en Espagne, en Colombie et au Pérou pour déployer, au nom de ses clients, les logiciels espions **Invisible Man** et **Night Crawler** [31, 32].

Recommandation concernant l'hameçonnage

- Ne pas cliquer sur les liens ou ouvrir les fichiers contenus dans des messages non sollicités.
- Être vigilant lors de l'ouverture de lien transmis *via* des *QR codes*.

Exploitation grâce à un accès physique au téléphone mobile

Certains attaquants peuvent chercher à profiter d'un accès physique aux appareils mobiles de leurs victimes pour les compromettre. Plusieurs cas de compromissions effectuées avec l'appui des forces de police locales ont ainsi été documentés par des éditeurs de sécurité. En Chine, des équipements mobiles ont ainsi été compromis par des logiciels espions comme **EagleMsgSpy** [33] ou **Massistant** [34]. En Iran, entre mars 2020 et mai 2023, l'éditeur de sécurité LOOKOUT a observé et documenté le déploiement de l'outil de surveillance **BouldSpy** à l'encontre d'au moins 300 équipements mobiles d'individus issus de minorités, possiblement par le commandement de la police de la République islamique d'Iran : la compromission initiale de la majorité des victimes aurait eu lieu à proximité de commissariats de police et de postes-frontières, suggérant que les téléphones auraient été confisqués puis compromis physiquement [35]. L'installation du logiciel espion **NoviSpy** sur les téléphones d'activistes serbes aurait également été perpétrée à la suite d'interrogatoires au poste de police. Dans ce dernier cas, le déverrouillage de certains téléphones aurait pu être réalisé en observant les codes de déverrouillage lorsqu'ils étaient saisis par les victimes [36].

L'accès physique à un terminal peut également permettre de collecter des informations nécessaires à la future compromission à distance d'équipements mobiles. Selon le service de sécurité de l'Ukraine (SBU), la préparation d'une campagne associée au MOA réputé russe Sandworm ciblant des appareils *Android* appartenant à l'armée ukrainienne aurait notamment été facilitée par l'analyse de téléphones récupérés sur le champ de bataille [37, 38].

Recommandation sur la protection physique du téléphone

- Ne pas connecter son téléphone à des prises USB ou appareils inconnus.
- Utiliser un bloqueur de données USB de confiance lors du chargement sur ce port.
- Protéger son code d'accès et préférer les codes d'accès composés d'au moins six caractères alphanumériques.
- Éteindre complètement son téléphone lorsqu'il est impératif de s'en séparer.

Par le piégeage du constructeur du matériel

Dans certains cas, les téléphones mobiles possèdent nativement des fonctionnalités considérées comme vulnérables ou potentiellement malveillantes. Le CERT lituanien a mis en évidence en septembre 2021 que plusieurs téléphones de la marque chinoise XIAOMI disposaient de fonctionnalités de censure préinstallées, interdisant aux utilisateurs certains termes en alphabet latin et en sinogramme sur des sujets potentiellement sensibles pour les autorités chinoises [19]. Même si ces capacités de censure étaient inactives, elles pourraient être réactivées

19. Les termes *Free Tibet*, *Democratic Movement* ou encore *Longing Taiwan Independence* étaient ainsi censurés.

à distance par le constructeur [39]. En 2025, KASPERKY a découvert des contrefaçons de téléphones de grandes marques vendues avec le code malveillant **Triada** préinstallé [40]. Ce dernier est conçu pour voler de données comme des identifiants de messagerie ou de la cryptomonnaie.

2.2.2 Exploitation des composants intégrés au système d'exploitation

Bien que bénéficiant généralement d'un haut niveau de sécurité dès leur conception, les fonctionnalités et composants intégrés aux terminaux, dont ceux issus de la chaîne d'approvisionnement, ne sont pas exempts de vulnérabilités et peuvent être détournés de leur fonction initiale par des attaquants. Ces composants intégrés au système d'exploitation sont d'intérêt pour les attaquants, du fait de leur présence sur une grande quantité d'appareils. Ce ciblage se traduit par l'exploitation de vulnérabilités ou le détournement de fonctionnalités et peut intervenir, en fonction du composant, à différentes étapes de la chaîne d'exploitation.

FIGURE 3 – Exemples d'exploitation des composants intégrés à l'OS sur les phases d'une chaîne d'exploitation

Les vulnérabilités présentes dans les fonctionnalités fournies par le système d'exploitation peuvent être employées au sein des chaînes d'exploitation. Plusieurs chaînes d'exploitation du logiciel espion **Pegasus** ont exploité des vulnérabilités jour-zéro [20] dans des fonctionnalités ou applications intégrées au système d'exploitation *iOS*, telles que *HomeKit* en 2024, *FindMy* en 2022 ou *Apple Wallet* [21] [41, 42, 43, 26]. De la même manière, en 2021, les opérateurs du MOA réputé russe Nobelium auraient ciblé des utilisateurs du système d'exploitation *iOS* à l'aide d'une chaîne d'exploitation d'une vulnérabilité dans le moteur de rendu *WebKit* [22], afin de récupérer des données d'authentification liées à des réseaux sociaux tels que *LinkedIn*, *Gmail*, *Facebook* et *Yahoo* [29, 44].

Ces fonctionnalités directement fournies par l'OS peuvent être détournées de leur fonction initiale par les attaquants notamment afin de bénéficier d'accès privilégiés au téléphone.

Aussi, les **fonctionnalités d'accessibilité**, initialement prévues pour faciliter l'usage du télé-

20. Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif au moment de son exploitation, aussi appelée vulnérabilité *0-day*.

21. La fonctionnalité *HomeKit* sert à contrôler les activités domotiques, *FindMy* à localiser un appareil, notamment en cas de vol, et *Apple Wallet* à gérer les cartes virtuelles.

22. Un moteur de rendu est un composant nécessaire à l'affichage de page Web. Sur *iOS*, *WebKit* est le moteur de rendu intégré au système et le plus répandu parmi les applications affichant des pages Web.

phone aux personnes en situation de handicap [23], peuvent être détournées pour obtenir des accès à certaines ressources comme le contenu affiché à l'écran ou les données saisies au clavier. Des codes malveillants cybercriminels, comme **Crocodilus**, mis en évidence en 2025, se basent sur ces accès pour récupérer par exemple des données bancaires et des cryptomonnaies [45].

D'autres **fonctionnalités internes**, comme celles à destination des développeurs, servent de base à des actions malveillantes. Par exemple, les chaînes d'exploitation des logiciels espions **Pegasus** ou **Triangulation** utilisaient un *framework* dédiés aux calculs mathématiques sur *iOS* pour déposer des implants [46, 47, 48].

Recommandations sur les fonctionnalités intégrées

- Ne pas accorder les permissions aux fonctionnalités d'accessibilité aux applications les demandant sans raison légitime.

Enfin, des composants tiers au téléphone mobile, intégrés par la chaîne d'approvisionnement du constructeur, peuvent également présenter des vulnérabilités susceptibles d'être exploitées comme vecteur initial pour compromettre l'équipement. Ces composants peuvent être matériels, tels que des puces dans l'équipement mobile, et être associés à des pilotes systèmes vulnérables, ou logiciels, comme les bibliothèques partagées (telles que *CoreAudio* sur *iOS* ou *Skia* sur *Android*). Ces composants externes, spécifiques et sophistiqués, sont présents sur les équipements de différents constructeurs et constituent donc des cibles de choix pour compromettre une grande diversité de téléphones mobiles.

> Parmi les briques tierces, le processeur de bande de base (*Baseband*) est une puce présente sur l'ensemble des périphériques mobiles. Ce processeur est nécessaire à l'interaction avec les réseaux de téléphonie mobile pour la gestion des protocoles radio. En 2023, AMNESTY INTERNATIONAL a décrit le module **Triton**, vendu par le consortium INTELLEXA, employé pour compromettre en zéro-clic des périphériques mobiles *via* l'exploitation de vulnérabilités spécifiques à leur processeur de bande de base. Ce module doit être utilisé conjointement avec un équipement type *IMSI catcher* pour compromettre la victime [4].

Par exemple, **les bibliothèques partagées, logiciels externes conçus pour faciliter le développement d'applications [24], sont régulièrement exploitées pour fournir un vecteur initial.** Parmi ces bibliothèques, celles dédiées aux fichiers multimédias (affichage d'image, lecture de vidéos) sont propices à des bogues logiques exploitables, du fait de la grande diversité de formats utilisés. En 2020, SAMSUNG a corrigé une vulnérabilité dans le codec *Qmage* et présente depuis 2014 [49]. Les vulnérabilités affectant les bibliothèques sont ainsi régulièrement intégrées à des chaînes d'exploitation, comme en 2023 avec le logiciel espion **Pegasus** [26].

Commentaire : ces bibliothèques partagées sont présentes sur tous les équipements disposant de la même version d'un système d'exploitation, et facilitent ainsi l'exploitation de vulnérabilités en offrant une surface d'attaque commune sur des modèles de terminaux différents. A contrario, la correction de vulnérabilités dans des applications utilisant ces bibliothèques implique pour les développeurs une forte dépendance aux fournisseurs de ces dernières.

Recommandation de mise à jour du système d'exploitation

- Appliquer les mises à jour du système d'exploitation dès qu'elles sont disponibles.

23. Les fonctionnalités d'accessibilité permettent par exemple d'énoncer vocalement le texte affiché à l'écran ou d'assister la saisie d'information dans les applications. Elles sont également disponibles pour les développeurs d'application pour les aider à rendre leurs applications plus accessibles.

24. Les systèmes d'exploitation intègrent directement des briques logicielles de codes dédiées, disponibles pour les développeurs d'application à travers des interfaces internes.

2.2.3 Exploitation des applications téléchargées par l'utilisateur

Les applications installées par l'utilisateur constituent une part importante de l'utilisation d'un équipement mobile. Elles sont téléchargées à travers un magasin d'applications, officiel ou alternatif, voire manuellement, sans passer par l'intermédiaire d'un magasin d'applications.

L'architecture des systèmes d'exploitation inclut nativement différents concepts de sécurité renforcée, tels que l'isolation des applications entre elles, l'instauration de permissions fines limitant l'accès aux différentes parties du terminal à l'instar des données utilisateurs, et un niveau restreint d'exécution par rapport au système.

> **Protection avancée de la mémoire**
>
> Dans les équipements informatiques, la gestion de la mémoire vive est souvent un vecteur de vulnérabilités liées à des erreurs introduites pendant le développement. Ainsi, afin d'éviter des utilisations non désirées de la mémoire vive, des mesures proactives, telles que MTE (*Memory Tagging Extension*) sur *Android* ou MIE (*Memory Integrity Enforcement*) sur *iOS*, ont été récemment mises en place par les constructeurs. Ces mécanismes permettent de limiter l'exploitation d'erreurs de gestion de la mémoire sous forme de vulnérabilités pouvant conduire à la compromission de l'équipement.

Ces mesures ne suffisent cependant pas à garantir une sécurité absolue. Les applications légitimes téléchargées par l'utilisateur sont également des logiciels dont les attaquants peuvent tirer parti.

Ces attaques peuvent inclure l'exploitation de vulnérabilités ou l'abus de fonctionnalités présentes dans l'application.

- **L'exploitation de vulnérabilités dans des applications légitimes téléchargées peut permettre de cibler simultanément les systèmes d'exploitation *Android* et *iOS*** à travers des fonctionnalités communes pour ensuite déployer des codes d'exploitation dédiés.
  En 2019, une vulnérabilité dans le traitement des appels sur *WhatsApp* (CVE-2019-3568) a permis de déployer le logiciel espion **Pegasus** avec le même vecteur initial sur des téléphones *Android* et *iOS* [42, 50]. De la même manière, en 2024, CITIZEN LAB a documenté le cas d'une vulnérabilité zéro-clic exploitée pour cibler l'application *WhatsApp* dans une campagne déployant le logiciel espion **Graphite** [25]. Les attaquants auraient ajouté les victimes sur un groupe *WhatsApp* puis envoyé un document PDF. Ce dernier était automatiquement traité par le téléphone de la victime, exploitant ainsi une vulnérabilité dans l'application et téléchargeant le logiciel espion [51].
  Commentaire : bien que les versions de l'application WhatsApp soient spécifiques à chaque système, les équipements Android comme IOS auraient été exposés à cette vulnérabilité. En effet, selon CITIZEN LAB, si la plupart des victimes recensées utilisaient un équipement Android, au moins un utilisateur iOS aurait été notifié d'une compromission par APPLE.

> **Recommandation concernant les applications non utilisées**
>
> - Désinstaller ou désactiver les applications qui ne sont pas ou ponctuellement utilisées.

- **Des fonctionnalités légitimes peuvent être directement utilisées dans des campagnes d'attaque.** C'est par exemple le cas de l'option de liaison entre un compte utilisateur d'application de messagerie et un appareil tiers, exploitée afin d'exfiltrer des conversations.
  En 2024, dans le cadre d'opérations de renseignement liées à l'invasion de l'Ukraine par la Russie, les MOA réputés russes UNC4221 et UNC5792 ont mené des campagnes d'ha-

25. Le logiciel espion **Graphite** est vendu par la société israélienne PARAGON.

meçonnage incitant les cibles à lier leur compte *Signal* à un appareil tiers [52]. En novembre 2024, une méthode similaire a été employée contre des cibles gouvernementales, diplomatiques, et de la recherche soutenant l'Ukraine par le MOA réputé russe Callisto, pour accéder à des comptes *WhatsApp* [28].

Les mécanismes de protection mis en place par les magasins d'applications pour détecter des comportements suspects peuvent être contournés pour charger du code malveillant. En 2025, KASPERSKY a découvert un code malveillant ayant pour objectif de voler des mots de passe de portefeuilles de cryptomonnaie. Ce code était intégré dans des applications [26] distribuées *via* le *PlayStore* pour *Android* et l'*AppStore* pour *iOS* [54].

> Certaines applications, bien que présentes sur des magasins officiels, peuvent exposer des données sensibles ou abuser des permissions demandées à l'utilisateur pour pouvoir récolter des données. Si ces applications sont moins intrusives qu'un logiciel espion, elles permettent cependant de collecter différentes informations comme la liste de contacts ou encore la géolocalisation des utilisateurs. Cette utilisation abusive de permissions a notamment été documentée par l'utilisation conjointe du micro et de la géolocalisation par l'application officielle de championnat de football espagnol afin de contrôler les diffusions publiques de matchs non déclarées [53].

Le déploiement du code malveillant peut être réalisé en téléchargeant le code malveillant *a posteriori* ou en piégeant les nouvelles versions d'une application légitime. Dans le premier cas, le code malveillant est absent de l'application installée et est téléchargé lors de son exécution. Cette technique a été utilisée par le code malveillant bancaire **SharkBot** [55]. Dans le second cas, une nouvelle version intégrant du code malveillant est téléchargée lors de la mise à jour de l'application [27]. C'est par exemple le cas du cheval de Troie **AhRat**, qui a été déployé *via* une mise à jour d'une application distribuée sur le *Google Play Store* en 2022, un an après la publication de l'application initiale [56].

Recommandations sur les permissions accordées aux applications

- Vérifier et gérer les permissions pour chaque application.

L'incitation à télécharger des applications présentant des portes dérobées est un autre un moyen utilisé par les attaquants pour compromettre des téléphones.

- **Certaines attaques informatiques visant des téléphones mobiles peuvent s'appuyer sur l'utilisation de fausses applications légitimes dont le nom a été usurpé.** Dans le cadre de campagnes observées par l'éditeur de sécurité LOOKOUT entre 2015 et 2019, les opérateurs du code malveillant **Monokle** [28] l'auraient distribué intégré dans des versions piégées d'applications populaires de messageries ou utilitaires [57]. De la même manière, entre 2014 et 2016, les opérateurs du MOA APT28, attribué au renseignement militaire russe, auraient distribué sur des réseaux sociaux regroupant des soldats ukrainiens une application militaire légitime dans une version altérée contenant la version *Android* du code malveillant **XAgent** [27, 58].

Recommandations concernant les sources d'installation des applications

- Ne pas installer d'applications en dehors des magasins officiels.

26. Par exemple, une application de livraison de repas propre aux Émirats arabes unis et à l'Indonésie.
27. Cette technique est également appelée *versioning*.
28. Le développement de cet outil est associé à l'entreprise russe SPECIAL TECHNOLOGY CENTER LTD. (STC).

- **Enfin, afin d'exercer des activités de surveillance intérieure, certains États imposent l'installation d'applications à leur population, lesquelles servent ensuite de portes dérobées vers les téléphones mobiles des utilisateurs.** Ainsi le gouvernement chinois imposerait l'installation d'applications à une partie ou à l'ensemble de sa population, à des fins potentielles de contrôle et de surveillance. C'est le cas par exemple de l'application *Xuexi Qiangguo* [29], imposée à l'ensemble des membres du Parti communiste chinois depuis le début de l'année 2019 et qui collecte de nombreuses données personnelles sur ses utilisateurs (localisation, habitudes de consommation, données de santé etc.) [59, 60].
  Dans d'autres pays, ces applications peuvent être imposées par un cadre règlementaire limitant les alternatives. En 2025, la Russie a approuvé le développement d'une application de messagerie par l'État. L'application *Max* est ainsi développée par VKONTAKTE, entreprise appartenant à la société d'État GASPROM [61]. Pour favoriser son utilisation, les fonctionnalités d'appels audio et vidéos d'applications comme *WhatsApp* ou *Telegram* ont été bloquées sur le territoire russe par l'agence de supervision des communications ROSKOMNADZOR. *Max* doit être préinstallée sur tous les téléphones mobiles vendus en Russie [62]. Bien qu'aucun code malveillant n'ait été identifié au sein de l'application, l'absence de chiffrement de bout en bout et les nombreuses données personnelles collectées pourraient ainsi permettre aux autorités d'utiliser *Max* comme outil de surveillance [63].

3 CAPACITÉS ET FINALITÉS DES ACTEURS CIBLANT LES ÉQUIPEMENTS MOBILES

3.1 Collecte de renseignement et surveillance

Si les opportunités de compromission d'équipements mobiles mentionnées précédemment (voir partie 2) peuvent être développées par des États possédant des capacités offensives avancées, l'essor du marché privé de la surveillance se confirme depuis les années 2010. Certaines entreprises fournissent des logiciels espions très perfectionnés à des gouvernements et leurs services de renseignement, d'autres offrent des capacités moins sophistiquées à travers des logiciels de traque (*stalkerware*) [30] à des entreprises et des particuliers.

3.1.1 Par des acteurs réputés étatiques

3.1.1.1 Développement ou achat des capacités mises en oeuvre

Les capacités d'exploitation d'équipements mobiles peuvent être développées par les services offensifs d'un État ou par délégation à son écosystème privé mais également par des entreprises étrangères spécialisées.

Ces entreprises financent d'importants projets de recherche et de développement. Des innovations régulières comme l'*ADINT* (voir 3.1.1.1) complexifient les chaînes d'exploitation et élèvent

29. Téléchargée plus de 100 millions de fois, son nom pourrait se traduire par « étudier et renforcer la nation ».
30. Un logiciel de traque peut être installé sur des appareils mobiles et permet à un tiers de surveiller l'emplacement de l'appareil et d'accéder aux messages, aux photos et à d'autres données personnelles à l'insu de l'utilisateur. L'installation de ces logiciels nécessite souvent un accès à l'équipement.

le niveau global de la menace. En employant des techniques et des capacités disponibles sur étagère, voire présentes dans l'écosystème cybercriminel, certains acteurs étatiques compliquent les processus d'imputation.

Enfin, dans certains pays, le recours à des Fournisseurs d'Accès Internet (FAI) dans des activités de surveillance interne facilite la distribution de logiciels espions en exploitant l'interception des communications directement depuis le cœur du réseau mobile.

En propre ou au sein de la chaîne de sous-traitance du pays

Les capacités offensives associées au ciblage d'environnements mobiles pour des opérations d'espionnage ou de surveillance peuvent être développées au sein de services étatiques ou par des prestataires faisant partie de l'écosystème national de LIO et vendant exclusivement à l'État client. C'est notamment le cas en Chine, aux Émirats arabes unis ou en Russie [27, 57, 68].

Cette internalisation des capacités témoigne d'une volonté de disposer de capacités en propre pour des questions de souveraineté, qui nécessitent des investissements financiers et humains conséquents.

À partir de 2014, le gouvernement émirien entre dans une dynamique de diversification des investissements en internalisant le développement de technologies jugées stratégiques pour la souveraineté nationale, notamment par la création de l'entreprise DARKMATTER. Cette société a été accusée par l'agence de presse REUTERS d'avoir contribué au ciblage d'activistes et d'officiels étrangers [68].

Ecosystème de sécurité offensive chinois

L'écosystème de sécurité offensive chinois s'intéresse particulièrement au développement de capacités ciblant les équipements mobiles. Il fonctionne avec un nombre important de prestataires de services qui travaillent comme fournisseurs pour les unités de cybercombattants de l'Armée populaire de libération (APL), du ministère de la Sécurité de l'État (MSE) ou du ministère de la Sécurité publique (MSP). De nombreuses entreprises comme la WUHAN CHINASOFT TOKEN INFORMATION TECHNOLOGY CO., LTD. ont développé des codes malveillants au profit d'opérateurs de MOA réputés chinois. Certaines, comme l'entreprise I-SOON, sont soupçonnées d'opérer directement ces MOA [33, 64].

Cet écosystème s'incarne aussi au travers d'équipes de recherches de vulnérabilités, comme celle de la Pangu Team, composée d'experts en sécurité offensive spécialistes des équipements mobiles, qui participe à des compétitions de recherche de vulnérabilités basées en Chine telles que la Tianfu Cup. Ainsi, lors de l'édition 2021, cette équipe est parvenue à exécuter du code à distance *via* un code d'exploitation 1-clic, sur un iPhone 13 Pro doté de la version 15 d'iOS [65].

Ce développement capacitaire est ensuite mis en oeuvre dans des campagnes d'attaques au moyen d'outils d'intrusion dédiés au ciblage d'équipements multi-plateformes. Les opérateurs du MOA BrazenBamboo, réputés chinois, auraient développé les codes malveillants de la famille **LightSpy**, adaptés au ciblage des systèmes d'exploitation *iOS*, *Android*, *Windows* et *macOS*, collectant la localisation de leurs cibles et procédant à l'enregistrement des appels téléphoniques VoIP [66, 67].

Achat de capacités auprès d'entreprises de LIOP

Si dans certains pays les entreprises de LIO sont intégrées dans la chaîne de sous-traitance d'État, d'autres entreprises, installées notamment en Europe, en Israël ou en Inde, vendent leurs prestations à un ensemble international de clients étatiques. Ces multiples ressources disponibles sur étagère facilitent et généralisent leur accès à des États ne disposant pas des technologies en propre ou souhaitant entraver le processus d'attribution [31].

Depuis les années 2010, ces sociétés spécialisées dans le développement et la vente de logiciels espions se sont multipliées à travers le monde.

31. En passant par des outils de surveillance développés et vendus par des entreprises privées plutôt que par des capacités internes, certains États souhaitent compliquer le travail d'identification de l'attaque. Toujours pour conserver son anonymat, un seul commanditaire peut utiliser plusieurs logiciels espions concomitamment ou successivement.

Certaines entreprises comme NSO GROUP et INTELLEXA fournissent des logiciels espions particulièrement intrusifs à travers un large panel de chaînes d'exploitation. Le logiciel espion **Pegasus**, a ainsi été observé à la fois dans des campagnes de distribution 1-clic notamment en Serbie ou au Mexique, mais également dans des campagnes sophistiquées où des vulnérabilités zéro-clic ont été employées [36, 74]. La chaîne d'exploitation choisie dépend du client et de ses ressources, mais également de la cible et de sa localisation [32].

Risques de dissémination de capacités offensives

L'entreprise HACKING TEAM, basée à Milan de 2001 à 2010, est à l'origine du développement de plusieurs logiciels offensifs comme **Galileo** [a], vendu à de nombreux États. En 2015, la divulgation par un hacktiviste de plus de 400 Go de données de l'entreprise a révélé la vente et l'utilisation de ces produits par des pays autoritaires à des fins de surveillance de la société civile.
La fuite des capacités de l'entreprise a également entraîné dans les jours et mois suivants l'exploitation de vulnérabilités jour-zéro sur le produit Flash Player d'ADOBE par des MOA réputés russes, chinois et nord-coréen [70]. Certains outils exfiltrés d'HACKING TEAM ont été employés par d'autres modes opératoires pendant plusieurs années, à l'instar de la plateforme de surveillance à distance **Galileo** : celle-ci a été réutilisée pour compromettre des cibles étatiques, notamment du personnel diplomatique, au moins entre 2016 et 2019 [71, 72]. Les opérateurs du MOA réputé russe Callisto auraient également utilisé un code malveillant issu de cette plateforme [72, 73].
La divulgation de capacités techniques d'une entreprise de LIOP peut donc entraîner une réutilisation des outils par d'autres acteurs et donc une élévation du niveau de la menace.

a. Selon les sources et les périodes, l'outil est également nommé **Da Vinci** ou **RCS** qui signifie *Remote Control System*[69].

L'écosystème israélien est aujourd'hui l'un des plus développés dans le secteur de la LIOP tant en nombre d'entreprises qu'en terme de capacités [75]. De nombreux membres de comités de direction des entreprises de cet écosystème proviennent des mêmes filières de formation qui servent également de vivier de recrutement [33]. Ces entrepreneurs du secteur cherchent à exporter leurs produits en créant des filiales à l'étranger, en s'associant à des entreprises étrangères, ou en utilisant des revendeurs situés dans des pays où la régulation est moins contraignante comme aux Émirats arabes unis. Les investisseurs étrangers sont aussi un maillon important dans le financement de cet écosystème pour accéder à de nouveaux marchés [78].

Prestations de courtiers en vulnérabilités

De nombreuses entreprises se sont spécialisées dans le développement et la vente de vulnérabilités jour-zéro à des acteurs offensifs. Ces intermédiaires, moins visibles, sont pourtant essentiels dans la chaîne d'approvisionnement de la surveillance numérique et sont implantés partout dans le monde.

Commentaire : ces sociétés de LIOP se développent notamment dans certaines régions du monde bénéficiant d'incitations fiscales attractives pour les sociétés et parfois d'un cadre réglementaire moins contraignant.

Les codes d'exploitation de ces entreprises pourraient également bénéficier à des acteurs réputés étatiques disposant de capacités en propre. Entre novembre 2023 et août 2024, les opérateurs du MOA réputé lié à la Russie Nobelium auraient utilisé des chaînes d'exploitation de vulnérabilités présentant des similarités avec celles déjà utilisées par les entreprises privées de surveillance INTELLEXA et NSO GROUP [44].

32. La présence de la cible dans un pays autre que le pays du client peut complexifier la mise en oeuvre de certaines compromissions, notamment celles impliquant la coopération d'entreprises de télécommunications locales.
33. Par exemple, l'unité 8200 de l'armée israélienne, spécialisée dans le renseignement technologique, est un vivier de recrutement dans l'écosystème israélien [76, 77].

Commentaire : la ressemblance entre ces chaînes d'exploitation met en lumière le risque de dissémination issu de la commercialisation large d'outils offensifs. Elle interroge par ailleurs sur la manière dont les opérateurs du MOA ont pu accéder à ces chaînes d'exploitation. Ils pourraient les avoir récupérées sur des téléphones compromis par INTELLEXA ou NSO GROUP, ou les avoir obtenus auprès du même fournisseur de vulnérabilités.

En novembre 2023 lors du Forum de Paris sur la Paix, la France et le Royaume-Uni ont lancé des consultations pour lutter contre la dissémination et l'usage irresponsable des outils offensifs commerciaux. Cette initiative, appelée Processus de Pall Mall depuis son lancement formel à Londres en février 2024, a mené à l'élaboration d'une doctrine de bonne conduite à destination des États [1]. Pour lutter contre ces menaces, elle encourage à la fois à une meilleure coopération des constructeurs pour renforcer la sécurité des équipements mobiles mais aussi à renforcer le partage d'informations sur les menaces observées tout en recommandant des cadres règlementaires encadrant l'utilisation et la vente de telles capacités.

Coopération ou compromission de courtiers spécialisés sur la vente de critères publicitaires (ADINT)

L'*ADINT* (contraction de *advertising* et *intelligence*) ou renseignement issu de publicité, se définit par la distribution massive ou spécifique d'annonces publicitaires vers une ou plusieurs cibles à des fins de profilage et de géolocalisation. Le système d'enchère de la publicité en temps réel met à disposition des annonceurs des critères identificateurs (âge, sexe, centre d'intérêt, localisation, catégorie socio-profesionnelle, etc.) leur permettant d'acheter, pour un public ciblé, des espaces publicitaires sur des sites internet ou des applications. Ce processus est exploité par les opérateurs de l'*ADINT*, qui, en usurpant le rôle des annonceurs auprès des plateformes d'enchères, collectent des critères à des fins de surveillance. Ces informations permettant à ces entreprises à la fois de cibler un individu avec précision et de récupérer des données de manière massive sur une population d'intérêt. Cette nouvelle technique de renseignement est en plein essor car encore très peu réglementée sur ses capacités offensives, et figure dans les brochures commerciales de nombreuses entreprises de LIOP [79, 80].

Les fournisseurs d'*ADINT* travailleraient en étroite collaboration avec des plateformes d'achat (DSP pour *Demand Side Platforms*) [34] ou auraient directement intégré ces capacités en interne [81, 82]. Ces coopérations ou l'intégration de ces capacités en interne permettent de ne pas dépendre d'un DSP autonome et ainsi de limiter les justifications de réutilisation de ces données et les risques de fuites.

Commentaire : au-delà de la coopération avec des entreprises détenant les critères identificateurs d'individus, la compromission de ces dernières par des États pourrait être une manière de récupérer ces informations pour mener des opérations à des fins d'espionnage ou de surveillance.

De plus, de nouvelles technologies basées sur l'*ADINT* seraient capables de compromettre des téléphones mobiles et des ordinateurs par la combinaison de l'envoi de publicité et de l'exploitation de vulnérabilités. Différents produits tels que **Sherlock**, **Patternz** ou **Alladin**, développés respectivement par les sociétés INSANET, ISA SECURITY et INTELLEXA, disposeraient de telles capacités [83, 84].

Recommandation sur la protection contre le profilage par publicité

- Supprimer l'identifiant de publicité ou le renouveler.

34. Ces plateformes d'achat détiennent les informations nécessaires au profilage des utilisateurs dans le système publicitaire

Recours à des Fournisseurs d'Accès à Internet (FAI)

Le recours aux Fournisseurs d'Accès Internet (FAI) facilite, pour des acteurs offensifs, l'interception des communications directement depuis leur réseau mobile.

Le logiciel espion **Predator** d'INTELLEXA peut ainsi être distribué à travers une compromission zéro-clic grâce au recours à un FAI local. Deux modules, nommés **Mars** et **Jupiter**, permettent respectivement de rediriger certaines communications d'une cible vers l'infrastructure attaquante et de récupérer les certificats et clés de déchiffrement. Ce dernier est positionné préalablement entre les serveurs desdits sites et les autorités de certifications, avec une collaboration de l'hébergeur, et transmet ainsi au module **Mars** les secrets nécessaires au déchiffrement des communications et leur modification [4]. La chaîne d'exploitation zéro-clic du logiciel espion **Predator** est illustrée par la Figure 4.

*Commentaire : selon les observations de l'ANSSI, un pays client du logiciel espion **Pegasus** aurait effectué en 2020 des redirections vers des copies malveillantes de sites légitimes grâce à la participation active d'un FAI dudit pays.*

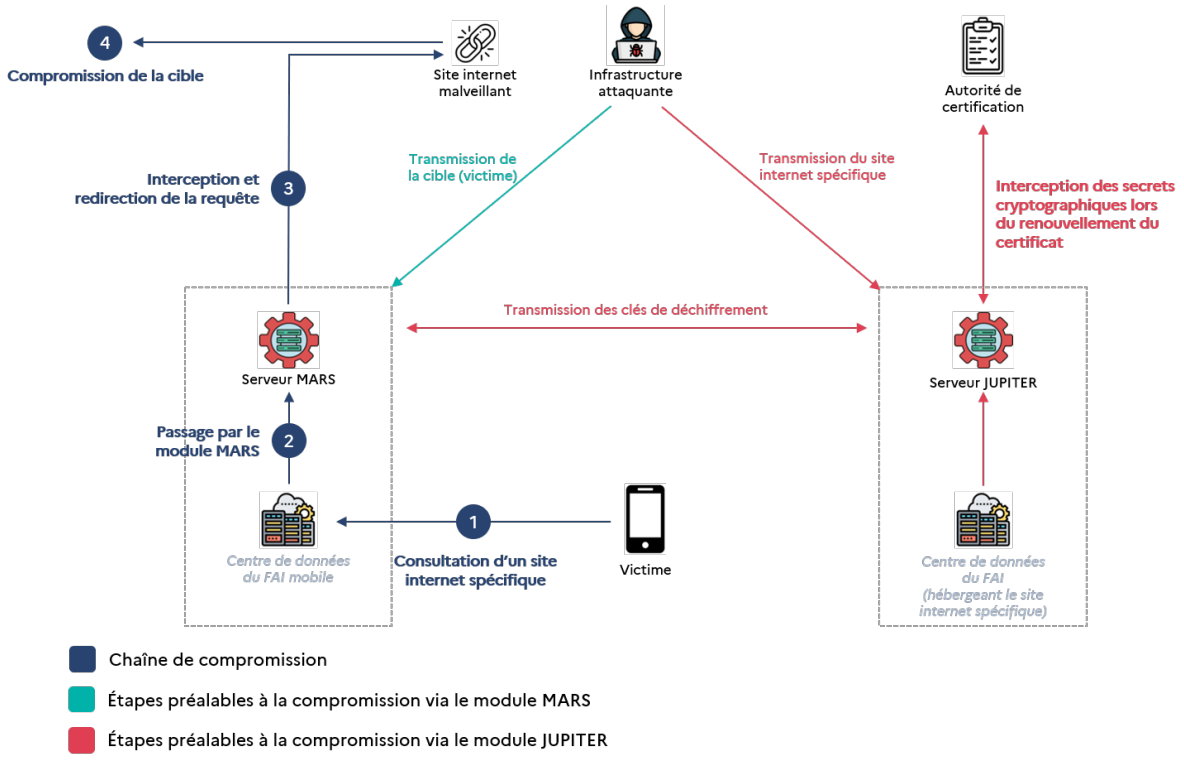

FIGURE 4 – Récapitulatif de la chaîne d'exploitation zéro-clic avec module **Mars** et/ou **Jupiter** en amont de la distribution du logiciel **Predator**

Au-delà du recours à des FAI locaux, certains acteurs offensifs abusent des faiblesses présentes dans les réseaux de télécommunications afin de faciliter le ciblage de leur victime finale. En 2022, l'entreprise TYKELAB, déclarée comme opérateur de communications et appartenant à l'entreprise de LIOP italienne RCS LAB, aurait ainsi utilisé de nombreux petits opérateurs, principalement situés dans des îles du Pacifique, pour envoyer un important volume de données vers des cibles dispersées à travers le monde. L'entreprise exploiterait des vulnérabilités qui permettent à des tiers de voir l'emplacement des utilisateurs de téléphones et d'intercepter leurs appels sans qu'aucune trace de compromission ne soit laissée sur les appareils [85].

Recommandation sur l'usage de téléphone mobile à l'étranger

- Lors de déplacements à l'étranger, il est recommandé d'appliquer les recommandations de ce document.
- En cas de déplacement sensible, il est recommandé d'utiliser un téléphone dédié.

Utilisation d'outils cybercriminels

Au cours de l'année 2024, des variants du cheval de Troie **Hydra** et de l'outil d'accès à distance ciblant les environnements *Android* **CraxsRat**, d'origine cybercriminelle, auraient été utilisés contre des cibles potentiellement militaires en Ukraine et associés à des MOA alignés sur des intérêts étatiques russes [30, 86].

Commentaire : l'utilisation de ces codes cybercriminels dans le cadre d'attaques à des fins d'espionnage témoigne d'une adaptabilité des attaquants à détourner des codes de leurs usages premiers. L'ANSSI n'a toutefois pas connaissance du chemin d'acquisition précis. Ils pourraient avoir été achetés ou obtenus de manière gratuite sur des places de vente ou forums cybercriminels.

3.1.1.2 À des fins d'espionnage ou de surveillance

L'ANSSI, ou d'autres membres du C4 selon le choix des personnes concernées, est régulièrement sollicitée pour analyser des suspicions de compromissions de téléphones d'individus à la suite de notifications à leurs utilisateurs provenant de constructeurs comme APPLE. Les postes occupés par les personnalités ciblées témoignent de campagnes visant à récupérer des informations sensibles sur les intérêts français. La réception dans certains cas de notifications à répétition par les mêmes usagers est caractéristique d'un ciblage précis.

Certaines campagnes d'espionnage d'environnements mobiles liées à des intérêts étatiques semblent coïncider avec la tenue d'évènements nationaux ou internationaux. Entre 2023 et 2024, le ciblage du gouvernement mongol par les opérateurs du MOA Nobelium pourrait entre autres être lié au contexte de la visite d'État de Vladimir Poutine en Mongolie en septembre 2024 [44, 87].

La compromission de téléphones mobiles de membres de comités de direction d'entreprises de secteurs stratégiques françaises par des logiciels espions sophistiqués a également été traitée par l'ANSSI.

En effet, les logiciels espions peuvent également être utilisés par différents acteurs offensifs dans le cadre d'espionnage économique ou industriel. Par exemple, entre février et juin 2023, 12 personnalités ou élus de l'Union Européenne en lien avec la régulation de la pêche illégale auraient été ciblés par des capacités associées en sources ouvertes au Vietnam [35] à travers les messages d'un faux compte *Twitter* [36] [88].

35. Le Vietnam, dont l'exportation de poissons rapporte plus de 750 millions d'euros chaque année, avait obtenu en 2017 un avertissement sous forme de carton jaune de l'Union Européenne en raison des efforts insuffisants effectués pour lutter contre la pêche illégale. Le vote d'un carton rouge par l'UE interdirait l'exportation du poisson vietnamien dans toute l'UE, ce qui représenterait pour le pays une perte importante de revenus [88].

36. L'attaquant répondait à des tweets avec le compte « @joseph_Gordon16 » en interpellant ses cibles et en joignant un lien qui menait vers un site Internet capable de compromettre les téléphones sur lesquels les cibles consultaient leur fil *Twitter*.

Recommandations sur l'usage en environnement professionnel

- Séparer les usages professionnels et personnels sur les équipements mobiles.
- En cas de discussion sur des sujets sensibles, placer les téléphones dans une autre pièce à une distance raisonnable.

Des campagnes d'espionnage d'environnements mobiles associées à des intérêts étatiques peuvent également s'inscrire dans le contexte de périodes conflictuelles de haute intensité. À titre d'exemple, dans le contexte de l'annexion de la Crimée en 2014 ou encore de la guerre déclenchée par la Russie contre l'Ukraine en février 2022, des opérateurs de MOA réputés liés à la Russie ou alignés sur ses intérêts auraient notamment ciblé des environnements mobiles liés aux forces militaires ukrainiennes [27, 52]. Ce ciblage se caractérise par l'utilisation significative de ce type d'environnement par les forces armées pour échanger des informations tactiques (communications militaires, données de géolocalisation, etc.).

Plusieurs MOA réputés liés à des États, comme la Chine, l'Iran ou la Russie, ont déjà été employés à l'encontre de minorités ethniques ou nationales et d'individus considérés comme des dissidents (ONG, journalistes, avocats, défenseurs des droits humains). Ainsi des MOA réputés liés à la Chine sont employés de manière récurrente et depuis plusieurs années pour cibler des individus considérés par le gouvernement chinois comme des dissidents ou des dangers pour la stabilité de son régime [89]. De même, CHECK POINT RESEARCH a révélé en février 2021 que le MOA Domestic Kitten (*alias* APT-C-50), réputé lié au gouvernement iranien, a ciblé depuis 2017, à l'aide du logiciel espion **FurBall**, plus de 1200 individus incluant des dissidents politiques, des soutiens de l'État islamique et des membres de la minorité kurde [90]. En 2021, une campagne similaire visant à déployer le logiciel espion pour *Android* **Pineflower** a été observée au moyen du MOA UNC788 [37], réputé lié au Corps des Gardiens de la Révolution Islamique (CGRI) [91].

Les logiciels espions sont aussi massivement utilisés pour cibler des journalistes ou des membres de la société civile. En 2025, CITIZEN LAB a révélé que le logiciel espion **Graphite**, développé par l'entreprise israélienne PARAGON, aurait compromis *via WhatsApp* des cibles en Italie. Un rapport parlementaire italien du 5 juin a établi la responsabilité des agences de renseignement italiennes dans l'utilisation de **Graphite** à l'encontre de deux représentants italiens de l'ONG MEDITERRANEA SAVINGS HUMANS [51, 92, 93].

3.1.2 Par des entreprises

Certaines entreprises de LIOP, comme l'entreprise israélienne BLACK CUBE, disposent de capacités peu sophistiquées, comparativement à celles précédemment citées, mais proposent notamment des logiciels espions ciblant des téléphones mobiles, notamment à des sociétés dans le cadre de contentieux judiciaires [94, 95]. D'autres disposent de moyens peu sophistiqués mais d'un vivier de personnels important, offrant ainsi une grande quantité de services à une clientèle allant de la grande entreprise à des cabinets spécialisés dans le renseignement d'affaires. Cette menace est aujourd'hui peu visible et donc largement sous-estimée et sous-évaluée.

L'entreprise indienne BELLTROX, fondée en 2013 et se présentant comme pratiquant du « *hacking* éthique », met à disposition de ses clients une grande quantité de compétences cyber offensives pour réaliser du renseignement d'affaires [96]. Ses clients seraient souvent des entreprises privées, principalement occidentales, qui souhaiteraient espionner des concurrents. Les

37. Ce MOA est également appelé TA453 ou APT42.

victimes sont nombreuses et issues de secteurs diversifiés : finance, industrie pharmaceutique, presse, énergie, principalement aux États-Unis et en Europe. En 2015, le dirigeant de BELLTROX, Sumit Gupta, aurait été mis en cause pour avoir compromis des comptes de messageries et des comptes *Skype* d'employés d'une entreprise américaine au profit d'un concurrent [97]. Le mode opératoire de l'entreprise est suivi en sources ouvertes sous le nom de **Dark Basin**. Ce MOA a été utilisé à l'encontre d'une victimologie extrêmement variée, caractéristique d'un MOA mercenaire. Plus de 13 000 cibles auraient été compromises de 2013 à 2020 [98].

3.1.3 Par des individus, dans le cadre de litige ou de vengeance

Un logiciel de traque, ou *stalkerware* est un logiciel pouvant être installé sur des appareils mobiles et qui permet à un tiers de surveiller l'emplacement de l'appareil et d'accéder aux messages, appels téléphoniques et profils de réseaux sociaux à l'insu de l'utilisateur.

Pour échapper au blocage par les magasins d'applications, ces logiciels sont vendus comme des outils de contrôle parental ou de contrôle d'activités des employés. Ces applications, qui devraient être installées avec l'accord de l'utilisateur, sont pourtant souvent paramétrées pour être discrètes et indétectables [38] [99]. En 2023, selon l'éditeur KASPERSKY, près de 31 000 utilisateurs de téléphones mobiles auraient été ciblés par un logiciel de traque dont environ 330 en France [100]. Ces logiciels sont notamment employés dans le cadre de violences intrafamiliales, en facilitant le contrôle coercitif des victimes par les auteurs de ces violences [101]. Leur installation, qui nécessite un accès physique à l'appareil, implique souvent que le harceleur appartienne au cercle familial, social ou professionnel de la victime.

Au-delà des problématiques d'atteinte à la vie privée et de consentement posées par l'utilisation de ces outils, ces logiciels ont souvent des failles de sécurité importantes alors même qu'ils stockent un nombre conséquent de données personnelles. L'éditeur ESET aurait ainsi détecté plus de 150 failles de sécurités dans 58 logiciels de traque pour *Android* qui pourraient avoir des conséquences sérieuses pour les victimes. La vulnérabilité observée la plus courante est la transmission des données de la victime vers le serveur du logiciel de traque à travers le protocole HTTP non sécurisé. Cela pourrait entrainer entre autres une attaque par AITM [99]. En cas de fuite de données de l'application, les données personnelles des victimes ainsi que des harceleurs pourraient également être divulguées. En février 2025, des millions de victimes des logiciels de traque **Spyzie**, **CocoSpy** et **Spyic**, ainsi que les messages, les photos, les journaux d'appels et d'autres données personnelles, ont été exposés du fait d'erreurs de développement [102, 103].

3.2 Autres finalités

L'ANSSI n'a pas à ce jour traité de compromissions de téléphones mobiles dont les finalités étaient lucratives ou à des fins de déstabilisation. Cependant, ces équipements restent des cibles de choix pour les cybercriminels qui peuvent exploiter les failles de ces équipements à des fins lucratives. Ce ciblage touche des particuliers et des entités de façon opportuniste sans spécificité de victimologie. Les attaques à des fins de déstabilisation *via* des équipements mobiles sont aujourd'hui peu nombreuses, mais leur effet direct sur la population demeure conséquent.

3.2.1 À des fins de déstabilisation

Plusieurs opérations de déstabilisation ont été menées par des groupes hacktivistes sur des équipements mobiles, notamment par la compromission d'API d'applications, afin de créer des si-

38. Il est plus compliqué d'installer ces outils sur *iOS* car le téléchargement d'une application requiert soit que le téléphone soit débridé soit de s'identifier avec le mot de passe du compte *iCloud* [99].

tuations de panique. Le 15 novembre 2023, le groupe *hacktiviste* pro-palestinien AnonGhost a annoncé *via* son canal *Telegram* avoir exploité une vulnérabilité dans l'interface de programmation d'application (API) de l'application israélienne *Red Alert*, qui notifie en temps réel ses utilisateurs des salves de roquettes et de missiles ciblant Israël. Cette compromission aurait permis à AnonGhost de diffuser de faux messages notifiant les 10 000 à 20 000 utilisateurs de l'application d'un bombardement nucléaire imminent sur le pays [39] [104].

En 2022, la compromission de l'application russe de mise en relation entre chauffeurs et particuliers *YandexTaxi* par le collectif *hacktiviste* Anonymous et le groupe *hacktiviste* pro-ukrainien IT Army of Ukraine avait conduit au rassemblement de tous les conducteurs de taxi de Moscou vers un bâtiment appelé « Hôtel Ukraine » [105]. Le ciblage de téléphones mobiles peut ainsi être utilisé pour engendrer des mouvements de foule, voire mettre en péril l'ordre public avec des mouvements de panique à des fins de revendications politiques.

3.2.2 À des fins lucratives

L'usage quotidien des équipements mobiles par leurs utilisateurs, combiné à la présence de nombreuses données à caractère personnel en font une cible de choix pour les attaquants cybercriminels [18]. Les codes malveillants destinés aux environnements mobiles ciblent principalement l'exfiltration de données bancaires permettant le détournement des fonds de la victime ou la revente des données à d'autres cybercriminels [106]. Les techniques de distribution de ces codes varient de la campagne d'hameçonnage à l'usurpation d'applications légitimes.

Les codes cybercriminels ciblant des équipements mobiles sont employés pour prendre le contrôle à distance du téléphone, enregister les frappes au clavier et intercepter les SMS, afin d'exfiltrer les identifiants d'application bancaires et de cryptomonnaies, à l'instar du code malveillant pour *Android* **Copybara** [107]. Ces identifiants sont par la suite détournés ou revendus [108, 106]. De même que pour les codes malveillants ciblant des environnements bureautiques, ces codes sont développés en propre ou disponibles *via* des services de revente [40].

Certains groupes cybercriminels identifiés pour avoir ciblé des environnements bureautiques saisissent également les opportunités d'attaques offertes par les environnements mobiles. L'acteur cybercriminel TA2727 a ainsi déployé en janvier 2025 les *infostealers* **LummaStealer**, **Marcher** et **FrigidStealer**, visant respectivement les environnements *Windows*, *Android* et *macOS* [109], à des fins de vol de couple identifiant-authentifiant.

Un téléphone mobile peut également servir aux attaquants pour compromettre dans un second temps un environnement informatique. Ainsi, depuis 2023, le groupe cybercriminel Scattered Spider cible les codes 2FA lors d'hameçonnages SMS ou vocaux sophistiqués afin de compromettre dans un second temps des systèmes d'information en effectuant de l'exfiltration de données et/ou en déployant un rançongiciel [20].

Commentaire : si à ce jour l'ANSSI n'a pas connaissance de compromission d'environnements bureautiques initiés par la compromission d'un équipement mobile, les nombreuses opportunités techniques mais aussi lucratives, par les données stockées, pourraient faire des téléphones mobiles une nouvelle cible de choix pour des acteurs malveillants. Il convient ainsi de maintenir un niveau de sécurité élevé lors de l'intégration d'une flotte mobile dans un parc d'entreprise.

39. L'attaque s'inscrit dans le cadre d'une campagne d'*hacktivisme* visant Israël et ses soutiens depuis le 7 octobre 2023.
40. Cette mise à disposition de codes cybercriminels est appelée *malware-as-a-service*.

4 RECOMMANDATIONS

Recommandations sur l'utilisation du protocole Wi-Fi

- **Désactiver complètement l'interface Wi-Fi** sur le téléphone lorsque ce type de réseau n'est pas utilisé, afin d'éviter des connexions à des réseaux Wi-Fi frauduleux.
- *Point d'attention : Sur iOS, la désactivation du Wi-Fi doit être effectuée en passant par l'application Réglages ; en effet, le paramétrage par le Centre de contrôles se limite à déconnecter le réseau sans désactiver l'interface Wi-Fi.*
- **Désactiver la connexion automatique aux réseaux connus** enregistrés dans le téléphone, y compris les réseaux privés.
- **Éviter autant que possible de connecter l'équipement mobile à des réseaux Wi-Fi publics**. Néanmoins, si cela est indispensable, il est nécessaire d'utiliser un VPN pour chiffrer les informations transitant par le réseau. Ce VPN doit s'appuyer sur des mécanismes de chiffrement tels que IPSec [a] ou TLS [b] et être maîtrisé par l'utilisateur, aussi bien côté client que côté serveur, pour garantir la confidentialité des échanges.

a. https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-ipsec
b. https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-tls

Recommandations sur l'utilisation du protocole Bluetooth

- **Désactiver l'interface Bluetooth** lorsque ce protocole n'est pas utilisé. À noter que sur *iOS*, la désactivation du Bluetooth doit être effectuée en passant par l'application *Réglages* ; en effet, paramétrage par le *Centre de contrôle* se limite à déconnecter les accessoires connectés sans désactiver l'interface Bluetooth.
- **Ne pas appairer l'équipement mobile à des dispositifs non maîtrisés ou partagés**, afin d'éviter toute exploitation ou fuite de données à travers ceux-ci.

Recommandation sur l'utilisation du protocole NFC

- **Désactiver l'interface NFC** de l'équipement permet d'éviter en cas de compromission de ce dernier qu'elle serve à capter les informations de cartes. La désactivation de l'interface NFC n'est possible que sur *Android*.

Recommandation sur l'usage de l'authentification multifacteurs

- **Verrouiller la carte SIM avec un code PIN** et **changer celui par défaut**. En effet, une carte SIM verrouillée et protégée par un code PIN ne peut pas être utilisée dans un équipement alternatif, ce qui limite la capacité d'un attaquant à récupérer des codes d'authentification à 2 facteurs (2FA)
- **Privilégier l'usage d'applications d'authentification** (***TOTP***) permet d'éviter la compromission de comptes en ligne dont l'authentification est à double facteur en cas de vol de carte SIM ou de *SIM-Swapping*

Recommandations concernant la sécurisation du système d'exploitation

Ces modes de durcissement des systèmes d'exploitation activent plusieurs limitations notamment sur les formats de médias, les liens contenus dans les messages ou encore les protocoles réseaux compatibles.
Point d'attention : l'activation de ces paramètres est recommandée pour toute personne à risque de ciblage par des menaces sophistiquées. L'activation de ces paramètres pouvant limiter certaines fonctionnalités utiles au quotidien [a], son activation peut être réduite à certaines périodes spécifiques (déplacement professionnel, séjour à l'étranger, climat politique ou commercial sensible).

- Sur *iOS*, le durcissement du système d'exploitation est disponible *via* le « *Mode Isolement* » [b]. Ce dernier est disponible depuis la version 16 d'*iOS*, sortie en 2022. Certaines fonctionnalités sont affectées comme les messages (blocage des pièces-jointes et des liens Internet), la navigation Web (restriction sur certaines technologies d'affichage et médias). Il reste cependant possible d'exclure manuellement certains sites Internet et application de ce mode pour ne pas en affecter l'utilisation.
- Sur *Android*, les fonctionnalités de durcissement sont appliquées par le « *Mode de Protection Avancée* » [c] présent depuis la version 16 d'*Android* sortie en 2025. Les fonctionnalités affectées sont les messages (passage dans des filtres anti-spam), verrouillage et redémarrage automatique du téléphone dans certaines circonstances et blocage des installations hors magasins officiels.

a. Par exemple, pour *iOS* et *Android* pour la connectivité Wi-Fi, la connexion aux réseaux ouverts ou à la sécurité obsolète n'est plus automatique et la désactivation de la 2G entraîne une absence de réseau lors d'un passage dans une zone uniquement couverte par de la 2G.
b. https://support.apple.com/105120
c. https://security.googleblog.com/2025/05/advanced-protection-mobile-devices.html

Recommandations concernant les applications de messagerie

- **Désactiver les applications de messagerie pré-installées si elles ne sont pas utilisées**, car ces dernières, de par leur présence sur tous les équipements mobiles, constituent un vecteur initial privilégié pour les attaquants.
- **Désactiver la réception automatique des messages de type MMS**, afin d'éviter le traitement de ces derniers sans action de l'utilisateur.
- **Éviter l'échange d'informations sensibles par SMS** et **préférer des messageries utilisant un chiffrement de bout en bout** afin de garantir la confidentialité des échanges.
- Désactiver la sauvegarde automatique des conversations de ces applications.

Recommandation concernant le redémarrage du téléphone

- **Redémarrer son téléphone**. L'arrêt complet du téléphone permet de fermer tous les processus et de supprimer tout logiciel s'exécutant uniquement en mémoire comme les logiciels espions sans persistance. Lors du démarrage du téléphone ces derniers ne pourront être exécutés. Cependant, la disparition du logiciel espion ne prémunit pas d'une réinfection par le même vecteur précédemment utilisé.
- **Éteindre puis rallumer son téléphone sans utiliser la fonctionnalité de redémarrage.** Certains logiciels espions parviennent à simuler un redémarrage du téléphone pour leurrer l'utilisateur.

Recommandation concernant l'hameçonnage

- **Ne pas cliquer sur des liens ou ouvrir les fichiers** présents dans des messages non sollicités. En cas de doute, il convient de vérifier la légitimité du message *via* un autre canal que celui par lequel a été reçu le message.
- **Être vigilant lors de l'ouverture de lien transmis *via* des *QR codes***. Les *QR codes* ne permettent pas d'identifier visuellement la destination d'un lien et peuvent être utilés par des criminels pour rediriger vers des ressources malveillantes.

Recommandation sur la protection physique du téléphone

- **Ne pas établir de branchement entre le téléphone et des équipements inconnus** [a].
- **Utiliser un bloqueur de données USB** de confiance en cas d'impératif de charger l'équipement sur un port USB inconnu. Ce dispositif permet de filtrer les connexions internes d'un port USB et de ne laisser passer que le courant électrique nécessaire à la charge de l'équipement. Ces dispositifs peuvent toutefois être vecteurs de pièges, il convient donc de ne pas utiliser ceux dont l'efficacité ne peut être vérifiée, tels que ceux offerts en marge de conférences.
- **Protéger son équipement avec un code d'accès robuste**. Les équipements mobiles imposent de plus en plus d'être déverrouillés pour initier des échanges de données *via* les ports physiques, un verrouillage robuste limite le risque de compromission par ce biais. Par extension, il est recommandé de **ne pas utiliser l'authentification biométrique** (reconnaissance faciale ou par empreinte digitale) afin d'éviter le déverrouillage sans besoin de connaissance d'un secret.
- **Éteindre complètement son téléphone** lorsqu'il est impératif de s'en séparer. En effet, lors du démarrage, de nombreuses fonctionnalités sont désactivées tant que le téléphone n'a pas été déverrouillé une première fois, réduisant ainsi la surface d'attaque.

Point d'attention : Le « Mode Protection Avancée » d'Android [b] *permet de désactiver l'USB et d'autoriser seulement la charge du téléphone lorsque ce dernier est verrouillé. Il en est de même par défaut sur iOS où la connexion à des accessoires USB n'est fonctionnelle que lorsque le téléphone est déverrouillé.*

a. Par exemple des bornes de recharge en libre service
b. Disponible depuis Android 16

Recommandations sur l'accès aux fonctionnalités d'accessibilité

- **Être vigilant lors des demandes d'autorisation d'accès aux fonctionnalités d'accessibilité** et, si l'application ne semble pas légitime, la **supprimer**.Les fonctionnalités d'accessibilité ne sont pas utilisables par les applications sans consentement explicite de l'utilisateur. Ce consentement se matérialise par l'affichage d'un message de confirmation lors du premier lancement de l'application.

Recommandation de mise à jour du système d'exploitation

- **Appliquer les mises à jour du système d'exploitation** dès qu'elles sont disponibles pour corriger les vulnérabilités affectant les composants et les mécanismes de sécurité.

Recommandation concernant les applications non utilisées

- **Désinstaller ou désactiver les applications qui ne sont plus utilisées ou utilisées de manière ponctuelle** (applications de voyage, liées à des évènements, jeux, réseaux sociaux, etc.). Ces dernières constituent une surface d'attaque inutile sur l'équipement mobile. Sur *iOS* et *Android* il est possible de supprimer le code logiciel tout en conservant les données de l'utilisateur :
- *iOS* : *Réglages* → *Général* → *Stockage de l'iPhone* puis cliquer sur chaque application à décharger et sélectionner l'option *Décharger l'app*.
- *Android* : *Paramètres* → *Applications* puis cliquer sur chaque application à archiver et sélectionner l'option *Archiver*.

Recommandations sur les permissions accordées aux applications

- **Vérifier les permissions accordées aux applications** installées sur l'équipement. Les versions récentes d'*Android* et *iOS* centralisent ces informations dans les paramètres de l'équipement :
  - *Android* : *Paramètres* → *Sécurité et confidentialité* → *Gestionnaire d'autorisations*
  - *iOS* : *Réglages* → *Confidentialité et sécurité*
- **Gérer les autorisations pour chaque application** lorsque cela est possible. De cette manière, si une autorisation ne semble pas nécessaire et n'empêche pas le fonctionnement de l'application, il convient de la retirer.
- **Éviter les applications semblant demander des permissions abusives** lors de la sélection d'une nouvelle application.

Recommandations concernant les sources d'installation des applications

- **Ne pas installer d'applications en dehors des magasins officiels**, notamment téléchargées directement ou en utilisant des magasins alternatifs. Ces magasins officiels, plus contrôlés, limitent la présence d'applications vérolées.

Recommandation sur la protection contre le profilage par publicité

Supprimer ou renouveler l'identifiant de publicité en effectuant les manipulations suivantes :

- Sur *Android* : *Paramètres* → *Sécurité et confidentialité* → *Autres paramètres confidentialité* → *Annonces* → *Supprimer l'identifiant publicitaire* ou *Rénitialiser l'identifiant publicitaire*
- Sur *iOS* : *Réglages* → *Confidentialité et sécurité* → *Publicité Apple* puis décocher *Annonces personnalisées*

Recommandation sur l'usage de téléphone mobile à l'étranger

- Lors de déplacements à l'étranger, il est recommandé d'appliquer les recommandations de ce document.
- En cas de déplacement sensible, il est recommandé d'utiliser un téléphone dédié.

Recommandations sur l'usage en environnement professionnel

- **Ne pas utiliser un équipement mobile personnel à des fins professionnelles**. Ainsi, même en cas de compromission de l'équipement personnel, aucune information professionnelle ne pourra être récupérée et utilisée par l'attaquant.
- **Exclure tout équipement électronique lors de discussions portant sur des sujets sensibles.** Les équipements mobiles doivent être laissés en dehors des salles de réunion. Par ailleurs, mettre l'équipement mobile hors ligne (par exemple en activant le « *Mode Avion* » n'est pas une mesure suffisante. En effet, cela n'empêche pas les logiciels espions de fonctionner en captant des conversations qui seront alors exfiltrées lors du retour du réseau.

Recommandations à destinations des entreprises

Ces recommandations s'adressent spécifiquement aux usages de terminaux professionnels

Gestion des terminaux

- **Gérer la flotte de terminaux professionnels à travers une solution de MDM** [a] et appliquer les recommandations de ce document. La gestion par une solution de MDM permet notamment de restreindre les applications installables et forcer l'installation des mises à jour.
- En cas de perte ou de vol, **effacer à distance le téléphone avec la solution MDM** afin d'éviter tout risque de latéralisation sur un réseau à partir des secrets qui peuvent y être configurés (certificats VPN, comptes de messagerie). Par ailleurs, les secrets doivent aussi être révoqués et renouvelés au niveau de l'infrastructure du réseau.

Bluetooth

- **Ne pas utiliser de dispositifs audio Bluetooth pour des communications sensibles.**

Wi-Fi

- **Mettre en place une liste de réseaux Wi-Fi autorisés à travers la solution de MDM utilisée** afin de limiter les risques de connexions à des réseaux non maitrisés.
- **Ne pas cacher le nom du réseau** (ou ESSID [b]) lors de la configuration des réseaux Wi-Fi, afin d'éviter des tentatives de connexions malveillantes.

Déplacement à l'étranger

- **Eviter d'utiliser les réseaux mobiles locaux** à l'étranger. Pour les communications vocales, **privilégier les « Appels Wi-Fi » à travers une connnexion VPN de type IPSec maîtrisée et les applications de messageries sécurisées** plutôt que des SMS.

a. *Mobile Devices Management*
b. *Extended Service Set Identification*

5 GLOSSAIRE

ADINT Contraction de *advertising* et *intelligence* ou renseignement issu de publicité, se définit par la distribution massive ou spécifique d'annonces publicitaires vers une ou plusieurs cibles à des fins de profilage et de géolocalisation. 18, 21

IMSI catcher Appareil ou dispositif technique qui, simulant le fonctionnement d'une antenne-relais de téléphonie mobile, capte et enregistre les IMSI des terminaux se trouvant à proximité avant de les transmettre à la station de base du réseau. 7, 15

stalkerware Un logiciel de traque peut être installé sur des appareils mobiles et qui permet à un tiers de surveiller l'emplacement de l'appareil et d'accéder aux messages, appels téléphoniques et profils de réseaux sociaux à l'insu de l'utilisateur. 18, 25

1-clic Chaîne de de compromission nécessitant une action de la part de l'utilisateur. 19, 20

2FA Authentification à double facteurs. 9, 26, 27

AITM Une attaque par *Adversary-in-the-middle* ou en français une attaque de l'homme du milieu consiste pour un attaquant à se glisser entre l'expéditeur et le destinaitre et à capter l'ensemble de leurs échanges. 6, 7, 25

antenne-relais Également appelées des stations de base. Équipements auxquels les terminaux se connectent pour accéder au réseau mobile. 6, 7

chaîne d'exploitation Succession d'exploitation de vulnérabilités permettant à un attaquant de prendre progressivement le contrôle d'un système. 8, 10–12, 14, 15, 18, 20–22

IMEI *International Mobile Equipment Identity*. Numéro unique permettant d'identifier les terminaux mobiles. 7

IMSI *International Mobile Subscriber Identification*. Numéro unique permettant à un réseau de téléphonie mobile d'identifier un usager. 7

jour-zéro Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif au moment de son exploitation, aussi appelée vulnérabilité *0-day*. 14, 20

LIO Lutte Informatique Offensive. Ensemble des actions menées par des acteurs étatiques dans le cyberespace consistant à infiltrer les systèmes d'information d'une organisation ou d'un individu pour les perturber, les modifier, les dégrader, les détruire ou en exfiltrer les données. 19

LIOP Lutte Informatique Offensive Privée. Ensemble des actions menées par des entreprises privées dans le cyberespace consistant à infiltrer les systèmes d'information d'une organisation ou d'un individu pour les perturber, les modifier, les dégrader, les détruire ou en exfiltrer les données. 3, 7, 8, 12, 20–22, 24

MOA Mode Opératoire d'Attaque. Ensemble cohérent de techniques, tactiques et procédures caractéristiques d'un attaquant ou d'un groupe d'attaquant. 9, 12, 13, 16, 17, 19–21, 23–25

OS *Operating System* ou système d'exploitation. 14

zéro-clic Chaîne d'exploitation de vulnérabilités ne nécessitant aucune action de la part de l'utilisateur. 10–12, 15, 16, 20, 22

6 RÉFÉRENCES

[1] Ministère de l'Europe et des Affaires étrangères. *Processus de Pall Mall : code de bonnes pratiques à destination des États, pour lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché (avril 2025)*. Avril 2025.
URL : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/processus-de-pall-mall-code-de-bonnes-pratiques-a-destination-des-etats-pour.

[2] Dare Abodunrin, Yoan Miche et Silke Holtmanns. *Some Dangers from 2G Networks Legacy Support and a Possible Mitigation*. Septembre 2015.
URL : https://ieeexplore.ieee.org/document/7346872.

[3] Libération. *SMS frauduleux et Imsi-catchers : les dessous d'une escroquerie dernier cri*. Juin 2025.
URL : https://www.liberation.fr/societe/police-justice/imsi-catchers-et-sms-frauduleux-les-dessous-dune-escroquerie-dernier-cri-20230423_TNQT6AJF65EGVP5BZBJ62VSQZM/.

[4] Amnesty International. *Predator Files : Technical Deep-Dive into Intellexa Alliance's Surveillance Products*. Octobre 2023.
URL : https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

[5] Bleeping Computer. *T-Mobile Says New Data Breach Caused by SIM Swap Attacks*. Décembre 2021.
URL : https://www.bleepingcomputer.com/news/security/t-mobile-says-new-data-breach-caused-by-sim-swap-attacks/.

[6] Al-Estiklal. *Tal Dilian — A Former Career IDF Intelligence Officer Turned Spy Technology Entrepreneur*. Juillet 2022.
URL : https://www.alestiklal.net/en/article/tal-dilian-a-former-career-idf-intelligence-officer-turned-spy-technology-entrepreneur.

[7] Intelligence Online. *Magen, la start-up qui chamboule l'interception Wifi*. Décembre 2015.
URL : https://www.intelligenceonline.fr/surveillance--interception/2015/12/16/magen-la-start-up-qui-chamboule-l-interception-wifi,108117226-art.

[8] Australian Federal Police. *Man Charged over Creation of 'evil Twin' Free WiFi Networks to Access Personal Data*. Juin 2024.
URL : https://www.afp.gov.au/news-centre/media-release/man-charged-over-creation-evil-twin-free-wifi-networks-access-personal.

[9] Legend. *Sébastien Lecornu, Ministre Des Armées : Attentats Déjoués, Tout Ce Qu'on Ne Sait Pas (Nucléaire, Etc.)* Mars 2025.
URL : https://www.youtube.com/watch?v=H0D4a_O_bxY.

[10] NRK. *Someone Could Be Tracking You through Your Headphones*. Septembre 2021.
URL : https://nrkbeta.no/2021/09/02/someone-could-be-tracking-you-through-your-headphones/.

[11] NOTUS. *War Zone Surveillance Technology Is Hitting American Streets*. Avril 2024.
URL : https://www.notus.org/technology/war-zone-surveillance-border-us.

[12] The New York Times. *In Stores, Secret Bluetooth Surveillance Tracks Your Every Move*. Juin 2019.
URL : https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

[13] The Walt Disney Company. *Privacy At The Walt Disney World Resort, The Disneyland Resort, And Aulani, A Disney Resort & Spa, And On Disney Cruise Line Vacations - Frequently Asked Questions About Bluetooth® Technology*. Avril 2023.
URL : https://privacy.thewaltdisneycompany.com/en/resortble/.

[14] Libération. *Les panneaux de pub du métro tracent-ils les téléphones des usagers ?* Mars 2019.
URL : https://www.liberation.fr/checknews/2019/03/25/les-panneaux-de-pub-du-metro-tracent-ils-les-telephones-des-usagers_1717316/.

[15] Armis. *BlueBorne Cyber Threat Impacts Amazon Echo and Google Home*. Novembre 2017.
URL : https://www.armis.com/blog/blueborne-cyber-threat-impacts-amazon-echo-and-google-home/.

[16] Oligo Security. *Airborne : Wormable Zero-Click RCE in Apple AirPlay Puts Billions of Devices at Risk*. Avril 2025.
URL : https://www.oligo.security/blog/airborne.

[17] Tristan Claverie et José Lopes Esteves. *BlueMirror : Reflections on Bluetooth Pairing and Provisioning Protocols*. Mai 2021.
URL : https://ieeexplore.ieee.org/document/9474325.

[18] WeLiveSecurity. *NGate Android Malware Relays NFC Traffic to Steal Cash*. Août 2024.
URL : https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/.

[19] Action Fraud Police UK. *Alert – How You Can Be Scammed by a Method Called SIM Splitting*. Septembre 2014.
URL : https://www.actionfraud.police.uk/alert/alert-how-you-can-be-scammed-by-a-method-called-sim-splitting.

[20] CISA. *Scattered Spider*. Novembre 2023.
URL : https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf.

[21] ANSSI. *État de la menace ciblant le secteur des télécommunications*. Décembre 2023.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/.

[22] Vice. *They Got 'Everything' : Inside a Demo of NSO Group's Powerful iPhone Malware*. Septembre 2018.
URL : https://www.vice.com/en/article/inside-nso-group-spyware-demo/.

[23] Google Project Zero. *A Deep Dive into an NSO Zero-Click iMessage Exploit : Remote Code Execution*. Décembre 2021.
URL : https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html.

[24] Kaspersky. *Operation Triangulation : iOS Devices Targeted with Previously Unknown Malware*. Juin 2023.
URL : https://securelist.com/operation-triangulation/109842/.

[25] Citizen Lab. *Sweet QuaDreams : A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers*. Avril 2023.
URL : https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[26] Google Project Zero. *Blasting Past Webp*. Mars 2025.
URL : https://googleprojectzero.blogspot.com/2025/03/blasting-past-webp.html.

[27] Crowdstrike. *Danger Close : Fancy Bear Tracking of Ukrainian Field Artillery Units*. Décembre 2016.
URL : https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[28] Microsoft Threat Intelligence Center. *New Star Blizzard Spear-Phishing Campaign Targets WhatsApp Accounts*. Janvier 2025.
URL : https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/.

[29] Google Threat Analysis Group. *How We Protect Users from 0-Day Attacks*. Juillet 2021.
URL : https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

[30] CERT-UA. *Attempts of cyber attacks on military systems using malware for mobile devices*. Septembre 2024.
URL : https://cert.gov.ua/article/6280563.

[31] META. *Adversarial Threat Report : Countering the Surveillance-for-Hire Industry & Influence Operations*. Février 2024.
URL : https://transparency.fb.com/sr/Q4-2023-Adversarial-threat-report.

[32] Wired. *This Secretive Firm Has Powerful New Hacking Tools*. Juin 2021.
URL : https://www.wired.com/story/phone-hacking-mollitiam-industries/.

[33] Lookout. *Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus*. Décembre 2024.
URL : https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware.

[34] Lookout. *Lookout Discovers Massistant Chinese Mobile Forensic Tooling*. Juillet 2025.
URL : https://www.lookout.com/threat-intelligence/article/massistant-chinese-mobile-forensics.

[35] Lookout. *Lookout Discovers Android Spyware Tied to Iranian Police Targeting Minorities : BouldSpy*. Avril 2023.
URL : https://www.lookout.com/blog/iranian-spyware-bouldspy.

[36] Amnesty International. *"A Digital Prison" Surveillance and the Suppression of Civil Society in Serbia*. Décembre 2024.
URL : https://securitylab.amnesty.org/latest/2024/12/a-digital-prison-surveillance-and-the-suppression-of-civil-society-in-serbia/.

[37] SBU. *SBU Exposes Russian Intelligence Attempts to Penetrate Armed Forces' Planning Operations System*. Août 2023.
URL : https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system.

[38] CISA. *CISA and International Partners Release Malware Analysis Report on Infamous Chisel Mobile Malware*. Août 2024.
URL : https://www.cisa.gov/news-events/alerts/2023/08/31/cisa-and-international-partners-release-malware-analysis-report-infamous-chisel-mobile-malware.

[39] Recorded Future. *Lithuanian Government Warns about Secret Censorship Features in Xiaomi Phones*. Septembre 2021.
URL : https://therecord.media/lithuanian-government-warns-about-secret-censorship-features-in-xiaomi-phones/.

[40] Kaspersky. *Triada : A Trojan Pre-Installed on Android Smartphones out of the Box*. Juillet 2025.
URL : https://www.kaspersky.com/blog/trojan-in-fake-smartphones/53331/.

[41] Citizen Lab. *Triple Threat : NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*. Avril 2023.
URL : https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/.

[42] Google Project Zero. *FORCEDENTRY : Sandbox Escape*. Mars 2022.
URL : https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html.

[43] Donncha O'Cearbhaill et Bill Marczak. *Exploit Archaeology : A Forensic History of in-the-Wild NSO Group Exploits*. Septembre 2022.
URL : https://www.virusbulletin.com/conference/vb2022/abstracts/exploit-archaeology-forensic-history-wild-nso-group-exploits/.

[44] Google Threat Analysis Group. *State-Backed Attackers and Commercial Surveillance Vendors Repeatedly Use the Same Exploits*. Août 2024.
URL : https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/.

[45] Threat Fabric. *Exposing Crocodilus : New Device Takeover Malware Targeting Android Devices*. Mars 2025.
URL : https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices.

[46] Kaspersky. *Operation Triangulation : The Last (Hardware) Mystery*. Décembre 2023.
URL : https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/.

[47] Amnesty International. *Forensic Appendix : Pegasus Zero-Click Exploit Threatens Journalists in India*. Décembre 2023.
URL : https://securitylab.amnesty.org/latest/2023/12/pegasus-zero-click-exploit-threatens-journalists-in-india/.

[48] Google Threat Analysis Group. *Buying Spying : How the Commercial Surveillance Industry Works and What Can Be Done about It*. Février 2024.
URL : https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

[49] Google Project Zero. *MMS Exploit Part 1 : Introduction to the Samsung Qmage Codec and Remote Attack Surface*. Juillet 2020.
URL : https://googleprojectzero.blogspot.com/2020/07/mms-exploit-part-1-introduction-to-qmage.html.

[50] Zimperium. *WhatsApp Buffer Overflow Vulnerability : Under the Scope*. Juin 2019.
URL : https://zimperium.com/blog/whatsapp-buffer-overflow-vulnerability-under-the-scope.

[51] CITIZEN LAB. *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*. Mars 2025.
URL : https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/.

[52] GOOGLE THREAT INTELLIGENCE GROUP. *Signals of Trouble : Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger*. Février 2025.
URL : https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger.

[53] ESET. *Spain's La Liga App Uses Fans' Phones to Detect Illegal Soccer Broadcasts*. Juin 2018.
URL : https://www.welivesecurity.com/2018/06/12/spains-la-liga-app-phones-detect-illegal/.

[54] KASPERSKY. *SparkCat Crypto Stealer in Google Play and App Store*. Février 2025.
URL : https://securelist.com/sparkcat-stealer-in-app-store-and-google-play/115385/.

[55] GOOGLE CLOUD. *Threat Horizons - August 2023*. Août 2023.
URL : https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf.

[56] ESET. *Android App Breaking Bad : From Legitimate Screen Recording to File Exfiltration within a Year*. Mai 2023.
URL : https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/.

[57] LOOKOUT. *Monokle*. Juillet 2019.
URL : https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf.

[58] ANSSI. *Ciblage et compromission d'entités françaises au moyen du Mode Opératoire d'Attaque APT28*. Avril 2025.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-006/.

[59] CURE53. *Analysis-Report "Study the Great Nation" 08.-09.2019*. Septembre 2019.
URL : https://cure53.de/analysis_report_sgn.pdf.

[60] CNN. *Chinese Communist Party Propaganda? There's an App for That*. Février 2019.
URL : https://www.cnn.com/2019/02/15/asia/china-xi-jinping-communist-party-app-intl.

[61] BBC NEWS. *Russia targets WhatsApp and pushes new 'super-app' as internet blackouts grow*. Septembre 2025.
URL : https://www.bbc.com/news/articles/ce9rj2145jgo.

[62] REUTERS. *Russia orders state-backed MAX messenger app, a WhatsApp rival, pre-installed on phones and tablets*. Septembre 2025.
URL : https://www.reuters.com/technology/russia-orders-state-backed-max-messenger-app-whatsapp-rival-pre-installed-phones-2025-08-21/.

[63] POLITICO. *Russia's answer to WhatsApp : Kremlin puts a spy in every new phone*. Septembre 2025.
URL : https://www.politico.eu/article/russia-app-max-data-privacy-concerns-whatsapp-kremlin-china/.

[64] NATTO THOUGHTS. *I-SOON : Another Company in the APT41 Network*. Octobre 2023.
URL : https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

[65] NATTO THOUGHTS. *The Pangu Team—iOS Jailbreak and Vulnerability Research Giant : A Member of i-SOON's Exploit-Sharing Network*. Février 2025.
URL : https://nattothoughts.substack.com/p/the-pangu-teamios-jailbreak-and-vulnerability.

[66] KASPERSKY. *iOS Exploit Chain Deploys LightSpy Feature-Rich Malware*. Mars 2020.
URL : https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/.

[67] VOLEXITY. *BrazenBamboo Weaponizes FortiClient Vulnerability to Steal VPN Credentials via DEEPDATA*. Novembre 2024.
URL : https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/.

[68] REUTERS. *'Karma' : Inside the Hack Used by the UAE to Break into iPhones of Foes*. Janvier 2019.
URL : https://www.reuters.com/investigates/special-report/usa-spying-karma/.

[69] VICE. *Hacking Team Gave Spyware Demos to Police Agencies Across the Nation*. Juillet 2015.
URL : https://www.vice.com/en/article/hacking-team-gave-spyware-demos-to-police-agencies-across-the-nation/.

[70] THE HACKER NEWS. *Zero-Day Flash Player Exploit Disclosed in 'Hacking Team' Data Dump*. Juillet 2015.
URL : https://thehackernews.com/2015/07/flash-zero-day-vulnerability.html.

[71] ESET. *New Traces of Hacking Team in the Wild*. Mars 2028.
URL : https://www.eset.com/gr-en/about/newsroom/press-releases-1/new-traces-of-hacking-team-in-the-wild/.

[72] BBC NEWS. *Hackers Targeted Foreign Office Data*. Avril 2017.
URL : https://www.bbc.com/news/technology-39588703.

[73] F-SECURE. *The Callisto Group*. Avril 2017.
URL : https://labs.withsecure.com/content/dam/labs/docs/callisto-group.pdf.

[74] CITIZEN LAB. *New Pegasus Spyware Abuses Identified in Mexico*. Octobre 2022.
URL : https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

[75] ATLANTIC COUNCIL. *Mythical Beasts and Where to Find Them : Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. Septembre 2024.
URL : https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

[76] CITIZEN LAB. *Hooking Candiru : Another Mercenary Spyware Vendor Comes into Focus*. Juillet 2021.
URL : https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[77] LE MONDE. *« Projet Pegasus » : comment la société israélienne NSO Group a révolutionné l'espionnage*. Juillet 2021.
URL : https://www.lemonde.fr/projet-pegasus/article/2021/07/19/projet-pegasus-comment-la-societe-israelienne-nso-group-a-revolutionne-l-espionnage_6088692_6088648.html.

[78] TECHCRUNCH. *Israeli Spyware Maker Paragon Bought by US Private Equity Giant*. Décembre 2024.
URL : https://techcrunch.com/2024/12/16/israeli-spyware-maker-paragon-bought-by-u-s-private-equity-giant/.

[79] INTELLIGENCE ONLINE. *L'ADINT, planche de salut du cyber israélien*. Mai 2023.
URL : https://www.intelligenceonline.fr/surveillance--interception/2023/05/26/l-adint-planche-de-salut-du-cyber-israelien,109977613-art.

[80] Intelligence Online. *Offensive ADINT Is Israeli Cyber Sector's New Secret Weapon*. Février 2024.
URL : https://www.intelligenceonline.com/surveillance--interception/2024/02/15/offensive-adint-is-israeli-cyber-sector-s-new-secret-weapon,110159842-eve.

[81] Forbes. *Exclusive : Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps*. Décembre 2020.
URL : https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/.

[82] Bloomberg. *Your Ad Data Is Now Powering Government Surveillance*. Mai 2023.
URL : https://www.bloomberg.com/news/articles/2023-05-11/surveillance-company-turns-ad-data-into-government-tracking-tool.

[83] Haaretz. *Israel Tried to Keep Sensitive Spy Tech Under Wraps. It Leaked Abroad*. Avril 2024.
URL : https://www.haaretz.com/israel-news/security-aviation/2024-04-11/ty-article/.premium/israel-tried-to-keep-sensitive-spy-tech-under-wraps-it-leaked-abroad/0000018e-c948-d480-a99e-cf5f24900000.

[84] Irish Council for Civil Liberties. *Europe's Hidden Security Crisis*. Novembre 2023.
URL : https://www.iccl.ie/digital-data/europes-hidden-security-crisis/.

[85] Lighthouse Reports. *Revealing Europe's NSO*. Août 2022.
URL : https://www.lighthousereports.nl/investigation/revealing-europes-nso/.

[86] Google Threat Intelligence Group. *Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives*. Octobre 2024.
URL : https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives.

[87] France 24. *La visite de Vladimir Poutine en Mongolie, "un pied de nez" lancé à la CPI*. Septembre 2024.
URL : https://www.france24.com/fr/europe/20240903-la-visite-de-vladimir-poutine-en-mongolie-un-pied-de-nez-lanc%C3%A9-%C3%A0-la-cpi.

[88] Mediapart. *L'incroyable puissance des armes de surveillance de Nexa et Intellexa*. Octobre 2023.
URL : https://www.mediapart.fr/journal/international/071023/l-incroyable-puissance-des-armes-de-surveillance-de-nexa-et-intellexa.

[89] Crowdstrike. *CrowdStrike 2025 Global Threat Report*. Février 2025.
URL : https://www.crowdstrike.com/explore/2025-global-threat-report.

[90] Checkpoint. *Domestic Kitten – An Inside Look at the Iranian Surveillance Operations*. Février 2021.
URL : https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/.

[91] Emiel Haeghebaert. *UNC788 : Iran's Decade of Credential Harvesting and Surveillance Operations*. Octobre 2021.
URL : https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf.

[92] The Guardian. *Italian Government Approved Use of Spyware on Members of Refugee NGO, MPs Told*. Mars 2025.
URL : https://www.theguardian.com/world/2025/mar/27/italian-government-approved-use-of-spyware-on-members-of-refugee-ngo-mps-told.

[93] CITIZEN LAB. *Graphite Caught : First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*. Juin 2025.
URL : https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/.

[94] THE GUARDIAN. *Ronan Farrow on Surveillance Spyware : 'It Threatens Democracy and Freedom'*. Novembre 2024.
URL : https://www.theguardian.com/tv-and-radio/2024/nov/23/ronan-farrow-surveilled-documentary.

[95] INTELLIGENCE ONLINE. *Black Cube au secours de Beny Steinmetz contre Vale*. Mai 2020.
URL : https://www.intelligenceonline.fr/renseignement-d-affaires_premier-cercle/2020/05/27/black-cube-au-secours-de-beny-steinmetz-contre-vale,108407256-bre.

[96] CITIZEN LAB. *Dark Basin : Uncovering a Massive Hack-For-Hire Operation*. Juin 2020.
URL : https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/.

[97] THE GUARDIAN. *Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones*. Décembre 2019.
URL : https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

[98] REUTERS. *Exclusive : Obscure Indian Cyber Firm Spied on Politicians, Investors Worldwide*. Juin 2020.
URL : https://www.reuters.com/article/technology/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1FI/.

[99] ESET. *Android Stalkerware Vulnerabilities*. Mai 2018.
URL : https://web-assets.esetstatic.com/wls/2021/05/eset_android_stalkerware.pdf.

[100] KASPERSKY. *Kaspersky 2023 Report on Stalkerware*. Mars 2024.
URL : https://securelist.com/state-of-stalkerware-2023/112135/.

[101] FRANCEINFO. *Des victimes de violences conjugales racontent le cyberharcèlement exercé par leur conjoint*. Août 2023.
URL : https://www.francetvinfo.fr/societe/violences-faites-aux-femmes/temoignages-j-etais-comme-une-bete-traquee-des-victimes-de-violences-conjugales-racontent-le-cyberharcelement-exerce-par-leur-conjoint_6005945.html.

[102] TECHCRUNCH. *Exclusive : Stalkerware Apps Cocospy and Spyic Are Exposing Phone Data of Millions of People*. Février 2025.
URL : https://techcrunch.com/2025/02/20/stalkerware-apps-cocospy-spyic-exposing-phone-data-of-millions-of-people/.

[103] TECHCRUNCH. *Spyzie Stalkerware Is Spying on Thousands of Android and iPhone Users*. Février 2025.
URL : https://techcrunch.com/2025/02/27/spyzie-stalkerware-spying-on-thousands-of-android-and-iphone-users/.

[104] CYBER NEWS. *Red Alert, Israel's Rocket Alert App, Breached*. Novembre 2023.
URL : https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/.

[105] HACKREAD. *Anonymous Hacked Russian Yandex Taxi App Causing a Massive Traffic Jam*. Septembre 2022.
URL : https://hackread.com/anonymous-russian-yandex-taxi-app-hacked/.

[106] INTEL 471. *Mobile Malware - Underground Perspective*. Novembre 2023.
URL : https://intel471.com/resources/whitepapers/mobile-malware-underground-perspective.

[107] ZSCALER. *Technical Analysis of Copybara | ThreatLabz*. Août 2024.
URL : https://www.zscaler.com/blogs/security-research/technical-analysis-copybara.

[108] TEAM CYMRU. *Coper / Octo : Team Cymru's Mobile Mayhem Conductor*. Mars 2024.
URL : https://www.team-cymru.com/post/coper-octo-a-conductor-for-mobile-mayhem-with-eight-limbs.

[109] PROOFPOINT. *An Update on Fake Updates : Two New Actors, and New Mac Malware*. Février 2025.
URL : https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware.

[110] ANSSI. *Hygiène numérique des téléphones mobiles*. Avril 2025.
URL : https://cyber.gouv.fr/publications/hygiene-numerique-des-telephones-mobiles.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

26 novembre 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr