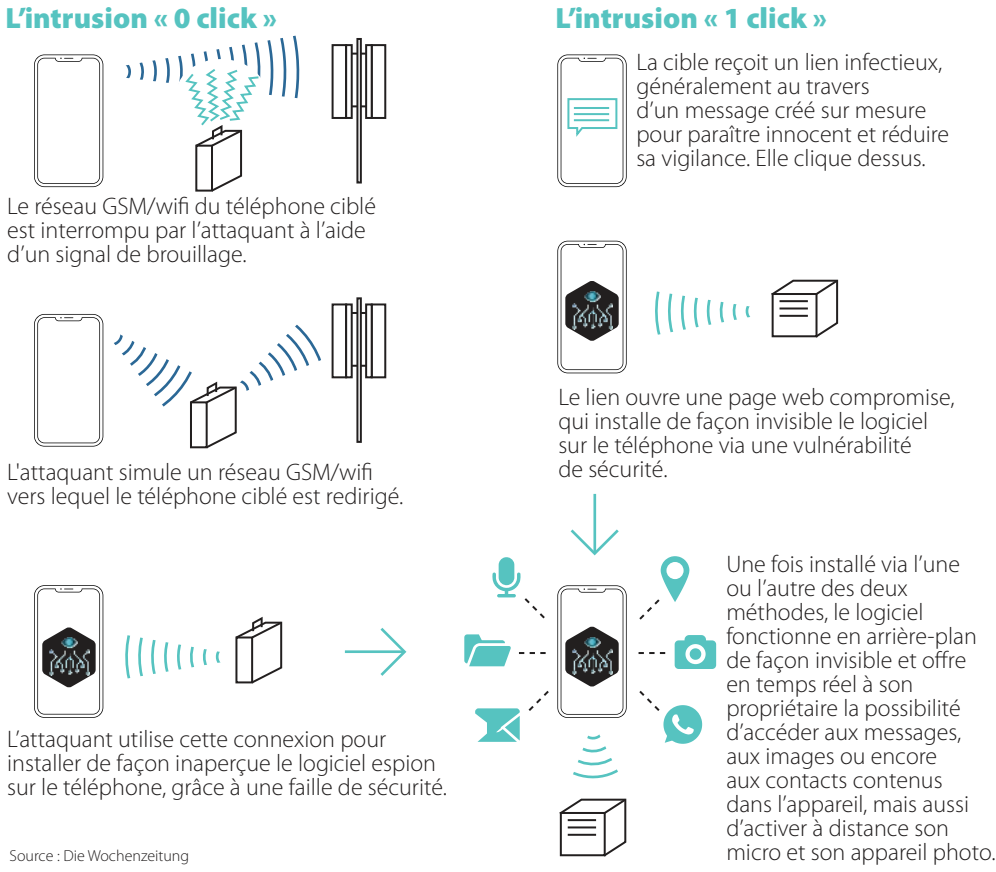
CYBERSURVEILLANCE

Predator Files

Le catalogue d'Intellexa, musée d'une cybersurveillance orwellienne

Grâce à de nombreux documents internes présentant les produits phares d'Intellexa, l'enquête Predator Files éclaire de façon inédite, avec l'aide du Security Lab d'Amnesty International, les capacités techniques redoutables des outils vendus par ce consortium à de nombreux Etats autoritaires.

Comment Predator peut s'introduire sur un smartphone



Source : Die Wochenzeitung

YANN PHILIPPIN ET JÉRÔME HOURDEAUX (MEDIAPART) AVEC ARTHUR SENTE

Il n'aura suffi que d'un clic pour que sa vie n'ait plus aucun secret pour les services secrets grecs. En 2021, le journaliste d'investigation grec Thanasis Koukakis, spécialiste des affaires de corruption qui touchent la classe politique de son pays, reçoit un message qui ressemble à celui d'une source désireuse de lui donner un bon tuyau : « Thanasis, avez-vous entendu parler de ce problème ? » En cliquant sur le lien inséré dans le message, Koukakis activera l'infection de son téléphone par le logiciel espion Predator, fabriqué par le groupe Intellexa. A l'ère d'internet et des smartphones, c'est comme s'il lui ouvrait la porte de toute sa vie privée et professionnelle.

De nombreux documents techniques confidentiels, obtenus par Mediapart et *Der Spiegel* dans le cadre de l'enquête Predator Files coordonnée par le réseau EIC (à laquelle a contribué *Le Soir*), et analysés avec l'aide du Security Lab d'Amnesty International, nous ont permis d'inventorier et de décortiquer les capacités des produits vendus par le groupe européen Intellexa et son partenaire français Nexa, unis au sein d'un consortium à partir de 2019.

Des outils dont la puissance est telle « qu'il est difficile, si pas impossible, de réconcilier leur usage avec les prescriptions en matière de droits humains », juge Amnesty International dans un rapport réalisé sur la base des documents partagés par l'EIC et publié ce vendredi.

Voici notre plongée dans le catalogue d'Intellexa, véritable musée moderne d'un cyberespionnage orwellien.

Le logiciel espion Predator, capable d'infecter les téléphones portables, est le produit phare d'Intellexa. Conçu par la société Cytrox (filiale d'Intellexa basée en Macédoine du Nord), il a été vendu par le groupe français Nexa sous le nom différent de Arrow. Des documents confidentiels de 2022 montrent également qu'Intellexa l'a rebaptisé Nova.

En somme, les produits vendus sous ces trois noms correspondent « globalement à la même technologie », selon une analyse réalisée par Amnesty International sur la base des documents obtenus par l'EIC.

Predator, le mouchard concurrent de Pegasus

Predator fonctionne sur le même principe que son concurrent Pegasus, de l'israélien NSO : il exploite des failles de sécurité (des erreurs dans le code informatique) présentes dans les deux systèmes d'exploitation faisant fonctionner l'immense majorité des téléphones : iOS (Apple) et Android (Google). Si besoin en achetant de telles failles auprès de hackers.

Même les téléphones les plus modernes ne résistent guère à Predator. Une présentation commerciale de juillet 2022 indiquait ainsi que Predator pouvait toujours infecter « les derniers appareils sous iOS et Android », dont l'iPhone 13 et le Samsung Galaxy S21, pourtant mis sur le marché un an plus tôt.

Une fois installé, Predator met littéralement sa victime à nu. Il peut récupérer l'ensemble des données du téléphone : sites web visités, courriels, messages (y compris ceux des messageries chiffrées comme Signal ou WhatsApp), et même « les mots de passe et certificats ». Le téléphone devient aussi un mouchard : Predator a accès à sa localisation, enregistre les appels et peut activer à distance le micro, l'appareil photo et la caméra.

Une fois le téléphone infecté, « tout se fait automatiquement, le logiciel envoie les données qu'il collecte toutes les 15 ou 30 minutes », nous a expliqué, sous couvert d'anonymat un ancien employé d'Intellexa qui a travaillé sur Predator. « Il est également possible d'envoyer une commande pour activer la caméra frontale et prendre un selfie », ajoute-t-il. « En fait, vous pouvez faire à peu près tout ce que vous voulez. Une fois que le client a acheté la licence, quelques clics suffisent. »

Les présentations commerciales précisent que Predator est « persistant », c'est-à-dire qu'il « survivra à l'arrêt du téléphone et son redémarrage ». En revanche, il « ne survivra pas à la réinitialisation » complète de l'appareil tel qu'il était à sa sortie d'usine.

Du « one click » au « zero click », grâce à Mars et AlphaSpear

A sa genèse, Predator fonctionnait uniquement sur base de l'infection dite « one click ». Autrement dit : la cible doit cliquer sur un lien malveillant pour l'activer. Intellexa parvient à générer de faux profils qui envoient les liens d'infection par e-mail, SMS, mais aussi « via WhatsApp, Telegram, Facebook et bien d'autres ».

Ce type d'attaque a le défaut de requérir un travail humain important, puisqu'il faut concevoir un message suffisamment crédible pour tromper la personne visée.

Notre enquête « Predator Files » révèle aujourd'hui qu'Intellexa a réussi à développer en 2022 une nouvelle technologie, baptisée Mars, capable d'infecter les téléphones via internet en mode « zero click », c'est-à-dire sans qu'aucune action de la cible ne soit requise.

Pour fonctionner, Mars nécessite la collaboration des opérateurs télécoms, priés d'installer à la demande de l'Etat client le système Mars au cœur de leur réseau. Raison pour laquelle la méthode d'intrusion ne fonctionne que dans un pays donné. C'est néanmoins un outil extrêmement puissant pour les services secrets, mais aussi pour les dictateurs, puisqu'ils peuvent infecter n'importe quel téléphone actif sur leur territoire.

Mais notre enquête révèle aussi qu'Intellexa et son partenaire français Nexa avaient déjà mis au point, dès 2019, une autre méthode d'injection de Predator en mode « zero click » : l'infection dite « tactique », ou « de terrain ».

Le principe : utiliser des appareils capables d'infiltrer, via les ondes radio, les téléphones situés dans un rayon de quelques centaines de mètres. Intellexa dispose de deux « vecteurs » différents : un appareil conçu par sa filiale Wispear, baptisé SpearHead, qui pénètre dans les téléphones via le wifi ; et un IMSI-catcher mis au point par Nexa, l'Alpha Max, qui utilise les réseaux cellulaires.

Comme tous les IMSI-catchers, l'Alpha Max dispose d'une antenne qui imite les antennes-relais des opérateurs mobiles. Lorsque la cible passe à proximité, elle « est discrètement déconnectée de son réseau original pour être connectée au réseau Alpha Max ». Dès lors « toutes les communications » vocales et SMS « sont enregistrées et conservées et la cible est géolocalisée », explique une plaquette de présentation de 2019.

Alpha Max peut se transformer en « vecteur d'infection », grâce à un agent baptisé Epsilon, capable d'intercepter et de modifier les données reçues par le téléphone, afin de déclencher l'infection par Predator lorsque l'utilisateur consulte un site web.

L'arme absolue d'Intellexa en matière de piratage « tactique » est une camionnette baptisée AlphaSpear 360. Equipée à la fois du SpearHead d'Intellexa et de l'Alpha Max de Nexa, elle peut infecter n'importe quel téléphone en mode « zero click » dans un rayon d'environ 500 mètres. Tarif : 9 millions d'euros pour la camionnette et les 100 premiers piratages, selon une offre commerciale de 2019.

Une plaquette de 2022 présente un autre système de piratage « zero click » à base d'IMSI-catcher, baptisé Triton. Il ne fonctionne qu'avec les téléphones Samsung, mais il est extrêmement discret et mobile : le système ressemble à un PC portable et tient dans une petite sacoche.

Cerebro, le big brother qui sait tout de vous

Cerebro fut le produit phare de Nexa pendant dix ans. Baptisé Eagle en 2007 lorsqu'il a été mis au point pour la Libye du colonel Kadhafi, le logiciel a été rebaptisé Cerebro en 2012, en référence à l'univers des comics X-Men.

Cerebro a été conçu au départ pour effectuer une surveillance de masse de la vie numérique de toute une population. Dans ses brochures, Nexa le présente comme « le premier système au monde » capable de surveiller internet « à l'échelle d'un pays entier ».

Concrètement, le système repose sur une sonde qui aspire le trafic internet, stocké ensuite dans Cerebro. Les opérateurs peuvent alors effectuer des recherches par mots-clés, identifier des cibles, puis avoir accès à toute leur activité, à la fois passée et présente : e-mails, consultations de sites web, activité sur les forums.

Nexa s'est ensuite diversifié, en développant des sondes et des appareils capables d'intercepter presque tous les types de communication : internet, communications vocales, téléphones satellites et réseau GSM, réseaux sociaux.

Les interceptions issues de ces différentes sondes sont transférées à Cerebro, qui les convertit dans un format unique et les analyse, pour aboutir à un panoptique offrant une « surveillance globale », comme le promet Nexa dans une brochure.

D'autant plus que Cerebro peut aussi se connecter aux bases de données gouvernementales afin d'y collecter des informations complémentaires.

Lors de leurs auditions dans le cadre de l'enquête judiciaire, les responsables de Nexa ont toutefois assuré que Cerebro était devenu progressivement aveugle, donc dépassé, en raison du chiffrement (ou cryptage) croissant des flux de données sur internet. Nexa a tenté de contourner le problème en s'intéressant davantage aux métadonnées des communications, ces données qui entourent le contenu principal.

A cette fin, le groupe a mis au point Jasmine puis IPDR (son évolution plus puissante), des modules de Cerebro permettant de connaître l'identité des interlocuteurs d'une cible et de détecter « les appels, les échanges de fichiers, ainsi que les envois de messages » (mais pas leurs contenus), même lorsque les gens utilisent des messageries chiffrées comme WhatsApp, Telegram ou Signal.