FUTURA

Ces apps pour espionner vos proches laissent fuiter vos données

Podcast écrit et lu par Emma Hollen

[*Générique d'intro, une musique énergique et vitaminée.*]

Des applis pour espionner vos proches qui se retournent contre vous, c'est l'actu de la semaine, dans Vitamine Tech.

[*Fin du générique.*]

Eh oui, vous avez bien entendu. Il existe des applis pour surveiller vos proches. Aujourd'hui il ne suffit plus de voir que votre moitié a reçu, lu et répond à votre SMS, de stalker ses snaps et de regarder discrètement par-dessus son épaule quand il ou elle tape un message ; rendues paranoïaques par la quantité phénoménale de secrets que peut receler un simple téléphone portable, certaines personnes se sont tournés vers des applications comme TheTruthSpy ou encore Copy9 pour prendre leurs proches en filature.

[*Une musique électronique calme.*]

Après les malwares et les ransomwares, voici les stalkerwares. Ces applications fleurissent à travers le monde et vous permettent d'espionner le portable de vos proches à distance. On y retrouve mSpy, SpyBubble, MinSpy ou encore CocoSpy. Oui, vous l'aurez compris, il y a un thème. Des apps grâce auxquelles vous pourrez suivre votre conjoint à la trace grâce à ses coordonnées GPS, mais pas seulement. Ainsi, TheTruthSpy vous permet également d'accéder à ses SMS, à son compte Facebook, Snapchat, Viber ou WhatsApp, à son historique, ses fichiers multimédia, ses contacts, ses apps, ou son journal d'appels, d'écouter ses appels, d'activer son micro pour écouter les conversations autour de lui, et de voir jusqu'aux touches de clavier sur lesquelles il appuie. Bref, si leur utilisation par la CIA ou la DGSI aurait déjà de quoi faire grincer des dents, mises entre les mains d'utilisateurs lambda, ces apps sont tout simplement dangereuses et représentent une atteinte grave à la vie privée. Bien évidemment, les stalkerwares sont pour la plupart illégaux et plusieurs ont été bannis des app stores d'Apple ou d'Android. Mais même s'ils ne se trouvent pas forcément sur les boutiques d'applications, ils restent relativement simples à télécharger et à déployer. Il vous suffit d'avoir accès au portable de la personne que vous souhaitez filer et d'y installer l'application de votre choix. Une fois activée, l'app est virtuellement indétectable, puisqu'elle n'apparaît pas sur l'écran d'accueil de la victime, et vous pouvez dès lors fouiner dans les moindres recoins de son appareil en toute impunité. On continue avec les mauvaises nouvelles ? Allez ! En plus de donner à vos proches paranos et à vos collègues mal intentionnés la possibilité d'accéder à l'ensemble de votre vie privée, il semblerait que

ces applications n’aient pas exactement la protection de vos données à cœur. Pas très surprenant pour des apps pirates, mais les chiffres n’en restent pas moins consternants. Ainsi, une récente enquête du média TechCrunch révèle que les éditeurs conservent la totalité des données collectées via leurs applications sur leurs serveurs : de vos messages à vos appels en passant par vos photos les plus intimes, tout est conservé durant des années contre seulement un an pour de nombreux services. Une pratique déjà répréhensible en elle-même et aggravée par le fait que lesdits serveurs sont loin d’être optimisés pour le stockage de datas aussi sensibles. C’est comme ça qu’une grosse faille de sécurité a permis à un groupe de hackers de récupérer des dizaines de gigaoctets de données provenant des mobiles espionnés. Des dizaines de gigaoctets, ça peut sembler peu quand on parle de vidéos ou de photos, mais souvenez-vous que les données les plus intéressantes sont les coordonnées GPS, les messages ou les fiches contact. Des fichiers dont le poids est négligeable et qui peuvent donc être collectés en grande quantité en requérant un minimum d’espace. En l’occurrence, ce sont les journaux d'appels, les SMS, les données de localisation et les mots de passe et données d'authentification à deux facteurs qui ont fuité des serveurs des applications TheTruthSpy, Copy9 et MxSpy. C'est donc la double peine pour les victimes qui, en plus d'avoir été espionnées à leur insu, voient leurs données personnelles circuler sur les réseaux des cybercriminels. Selon le rapport de TechCrunch, les victimes viennent des quatre coins de la planète et l’on en retrouverait dans presque tous les pays. La fuite aurait eu lieu en avril de cette année et concernerait pas moins de 360 000 appareils. Quant aux stalkers à l’origine de ces installations, ils seraient environ 337 000 à travers le monde. Alors comment éviter de tomber dans le piège ?

[*Virgule sonore, une cassette que l’on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

Notez d’abord que l'essentiel des mobiles touchés par ce phénomène sont des Android, sur lesquels il est possible de forcer l'installation d'une application qui n'a pas été téléchargée directement sur le store. Le premier réflexe à avoir consiste donc à faire le tour de l’ensemble des apps téléchargées et installées sur le smartphone pour supprimer celles qui ne sont pas utilisées et en particulier celles que vous ne vous souvenez pas d’avoir installées. Mais il y a également d’autres indicateurs comme une batterie qui se décharge plus vite que d’habitude. L’application a en effet pour rôle de télécharger vos données pour les envoyer à votre espion. Une opération gourmande en consommation de données qui a tendance à drainer l’énergie de votre portable. On remercie également les journalistes de TechCrunch qui ont créé un outil en ligne permettant de vérifier si votre mobile fait partie de la base de données ayant fuité en avril dernier. Si vous avez un doute, n’hésitez donc pas à vous rendre sur leur page pour y entrer le numéro IMEI de votre portable ou l’identifiant publicitaire de votre tablette. Le premier s’obtient en tapant *#06# sur votre mobile, et le second en suivant le chemin Paramètres, Options de Confidentialité puis Annonces sur votre tablette. En France, il existe par ailleurs une coalition anti-stalkerwares. Elle s’adresse essentiellement aux femmes victimes de violences conjugales et qui sont susceptibles d'être espionnées à leur insu par leurs partenaires. Pour détecter l’application malveillante sur leurs smartphones, le tribunal judiciaire de Paris utilise une tablette baptisée Veriphone. Si un stalkerware est détecté, l’infraction est ajoutée au dossier de plainte. Enfin, si le doute subsiste et que vous préférez ne courir aucun risque, la meilleure solution est encore de réinitialiser votre portable, mais ça, on ne le souhaite qu’aux personnes qui ont vraiment quelque chose à se reprocher.

[*Virgule sonore, un grésillement électronique*.]

C’est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, rendez-vous sur vos apps audio préférées pour vous abonner à ce podcast, et n’hésitez pas à nous laisser une note et un commentaire pour soutenir notre travail. Cette semaine je vous invite à découvrir notre nouveau podcast Jeunes Pousses, dédié à l’innovation positive ou tech for good. Le premier épisode sort demain, jeudi 3 novembre, alors n’hésitez pas à aller vous abonner sur vos plateformes d’écoute préférées dès maintenant. Pour le reste, je vous souhaite une excellente journée ou une très bonne soirée, et je vous dis à la semaine prochaine, dans Vitamine Tech.

[*Un glitch électronique ferme l’épisode*.]