FUTURA

Coupez vos appareils ! Le Bluetooth pourrait coûter l’indépendance du Groenland ?!

Podcast écrit et lu par Adèle Ndjaki

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

Le Bluetooth est-il un danger invisible qui menace le Groenland ? C'est le décryptage de la semaine dans *Vitamine Tech*.

[*Fin du générique.*]

Serait-ce la panique? Le Danemark vient de demander à ses fonctionnaires au Groenland de couper le Bluetooth sur tous leurs appareils afin de prévenir tout risque d'espionnage. Comment un simple signal sans fil peut-il s’inscrire dans des enjeux de sécurité et de rivalités géopolitiques? Bonjour à toutes et à tous, je suis Adèle Ndjaki et cette semaine dans *Vitamine Tech* on décrypte le pouvoir du bluetooth.

[*Une musique électronique calme.*]

Il se trouve dans nos téléphones, nos écouteurs, nos montres connectées et parfois même dans nos claviers ou nos voitures. Le bluetooth est partout. C’est pratique, discret et pourtant, il émet en permanence de petits signaux radio autour de vous, même quand vous ne l’utilisez pas activement. Et ça, ça pose un grand problème dans certaines circonstances. Et si je vous disais par exemple que cette fonctionnalité pourrait coûter l’indépendance du Groenland, me croiriez-vous? Depuis quelques jours, le gouvernement danois a diffusé une consigne très claire auprès de ses fonctionnaires groenlandais : désactiver le Bluetooth sur tous les appareils, professionnels comme personnels. Donc on parle là des smartphones, casques audio, portables, tablettes, et ce, quelle que soit la marque, car la directive ne cible aucun fabricant en particulier. Apple, Samsung, Sony et toutes les autres enseignes ne sont accusées de rien dans cette histoire. En fait, il faut comprendre que tout appareil émettant un signal Bluetooth peut devenir une source d’information exploitable. Dans un territoire stratégique comme le Groenland, un territoire autonome rattaché au Danemark qui est par la même occasion un espace géopolitique sensible par rapport à ses ressources naturelles et ses routes maritimes, ces signaux peuvent permettre la localisation, l’identification ou l’observation indirecte de personnels et d’équipements, même sans piratage direct. Dans ce contexte, toute émission radio peut devenir un point d’observation pour un acteur très ambitieux. Alors, l’objectif de cette mesure n’est pas de dire que chaque appareil est compromis, mais plutôt de réduire tout risque évitable. Pour les fonctionnaires et agents

travaillant dans des zones stratégiques, désactiver le Bluetooth devient un geste élémentaire de prudence au même titre que chiffrer ses communications ou éviter les réseaux Wi-Fi publics.

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

Malgré son image de technologie simple et pratique, le Bluetooth a régulièrement révélé des failles de sécurité depuis sa création. Certaines ont été étudiées ou exploitées dans des démonstrations de chercheurs en sécurité pour montrer comment un signal Bluetooth peut devenir un point d'entrée sur un appareil. Le principe est simple : tout appareil équipé d'un Bluetooth émet un signal radio. Selon sa configuration, sa mise à jour logicielle ou le contexte dans lequel il est utilisé, ce signal peut parfois être détecté et, dans certaines conditions, exploité pour interagir avec un appareil à l'insu de l'utilisateur. Deux techniques sont souvent citées : le bluebugging, qui permettait par le passé d'accéder à certaines fonctions d'un téléphone à distance, ou le bluesnarfing, qui cible plutôt les données stockées sur l'appareil, comme les contacts ou les fichiers. Mais aujourd'hui, ces attaques concernent surtout des appareils anciens, mal configurés ou non mis à jour. En fait, tout appareil qui émet un signal peut devenir un point d'exposition dans un environnement sensible. Et ce risque ne concerne pas que les smartphones. Les écouteurs et casques sans fil, souvent allumés en permanence, émettent eux aussi des signaux continus. Certains systèmes de connexion rapide peuvent permettre à une personne malintentionnée qui se trouve proche de vous de détecter votre appareil, de l'identifier de façon unique et de suivre sa réapparition dans le temps. Même sans accéder au contenu, ces informations peuvent suffire à déduire des habitudes, des déplacements ou la présence de personnes dans une zone donnée, ce qui constitue un problème de sécurité. Et dans certains cas, ces échanges révèlent aussi des métadonnées techniques : le type d'appareil, sa version logicielle, ou son comportement radio, des données qui peuvent devenir intéressantes dans un contexte de renseignement. Pour corriger ces vulnérabilités, les fabricants publient régulièrement des mises à jour. Mais entre la découverte d'un problème, la publication d'un correctif et son installation réelle sur les appareils, du temps peut s'écouler et pendant ce laps de temps, certains équipements restent exposés. La faille de sécurité BlueBorne, découverte en 2017, l'a bien montré. Elle touchait plusieurs systèmes différents et provenait d'une faiblesse du protocole bluetooth lui-même. Ce cas montre qu'une même faille peut toucher des appareils très différents et que sa correction dépend de nombreux acteurs. Mais soyez rassuré, dans la vie quotidienne, il est très rare d'être confronté à ce type d'attaque. En revanche, dans les environnements sensibles comme l'administration, les postes diplomatiques ou les sites militaires, les autorités recommandent souvent de limiter les signaux émis par les appareils électroniques. Cette précaution s'appuie sur les vulnérabilités documentées et sur le principe de réduire toute surface d'exposition potentielle. C'est dans ce cadre que le Danemark a demandé à ses fonctionnaires au Groenland de désactiver le Bluetooth sur leurs appareils. Donc que faut-il retenir de cet épisode ? Qu'au final, l'affaire du Groenland rappelle une chose simple : même les technologies les plus banales peuvent être utilisées pour obtenir des informations. Pour protéger ses informations sensibles, la première étape reste de faire attention aux appareils que l'on utilise tous les jours.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de *Vitamine Tech.* Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le tout nouvel épisode de Bêtes de science dans lequel Agatha Liévin-Bazin vous fait plonger dans les profondeurs de la mer Rouge afin de vous présenter la murène géante, un animal d'une ingéniosité époustouflante! Pour le reste, je vous souhaite tout le meilleur, et comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

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