FUTURA

Cybersécurité : les ampoules connectées représentent aussi un danger !

Podcast écrit et lu par Adèle Ndjaki

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

Le hackage par ampoules connectées, c'est l'actu de la semaine dans vitamine Tech !

[*Fin du générique.*]

Contrôler l'éclairage, le chauffage ou encore la sécurité de sa maison en un clic sont autant d'options proposées par la domotique aujourd'hui. Mais en parallèle, ce marché est aussi devenu l'un des terrains de jeu préférés des hackers depuis pas mal d'années. Grâce aux systèmes intelligents, les pirates peuvent maintenant avoir accès à nos données privées en se connectant à toutes les sortes d'objets comme des enceintes ou encore des ampoules connectées. Et justement, étant l'un des produits les plus faciles à cracker, cette petite boule lumineuse présente dans toutes les pièces d'un foyer ou d'une entreprise serait devenue l'un des objets les plus utilisés pour pirater, ce qui est particulièrement inquiétant.

[*Une musique électronique calme.*]

Mi-septembre 2016. L'hébergeur OVH cloud, connu pour être le plus gros hébergeur européen est victime d'un piratage de très grande ampleur. Pour la première fois de son histoire, l'entreprise française subit une attaque menée par des objets connectés. Des pirates se sont servis de caméras pour rendre inaccessible le serveur de la société en submergeant de données inutiles le réseau de l'entreprise pour le bloquer. Les auteurs de l'assaut auraient réussi à exploiter plus de 140 000 caméras en simultané, ce qui aurait constitué à l'époque la plus grosse attaque en déni de service jamais enregistrée. Et donc vous l'aurez compris, si les objets connectés nous offrent la possibilité de contrôler à distances le matériel en notre possession et ainsi de nous rendre la vie plus facile, il est cependant établi depuis de nombreuses années qu'ils représentent aussi un danger pour notre vie privée. Je vous en parlais d'ailleurs dans un épisode de Vitamine Tech dans lequel j'explique la façon dont la domotique est utilisée comme arme dans les violences domestiques. Un triste constat qui vient démontrer que n'importe qui à la possibilité de pirater un objet intelligent, et ce, à cause de leur essence même : la connexion de ces matériaux au Wi-Fi les rendrait plus vulnérables au hacking, permettant aux pirates de prendre le contrôle de tous nos réseaux. Mais la faille se présenterait aussi dès l'élaboration de ces appareils qui ne seraient pas vraiment dotés de systèmes sécurisant les données privées. La course à l'innovation étant lancée depuis plusieurs années,«les aspects liés à la sécurité ralentiraient [d'après Renaud Lifchitz, expert en sécurité informatique], la sortie du

produit et représenteraient des coûts supplémentaires.» , ce qui expliquerait en grande partie les raisons qui poussent les concepteurs d'objet connecté à ne pas vraiment s'appliquer en ce qui concerne le système de sécurité de leur production. D'ailleurs, des chercheurs de l'Université di Catania en Italie, et de l'Université de Londres auraient récemment décelé quatre grandes failles de sécurité dans les ampoules connectées TP-Link Tapo L530E, l'une des marques d'ampoules les plus vendues au monde, ainsi que dans l'application qui leur est associée. La plus grande faiblesse résiderait dans la résistance du dispositif de contrôle censé garantir la sécurité des communications entre l'ampoule et les autres appareils permettant ainsi aisément d'usurper l'identité de l'ampoule. Et ce n'est vraiment pas une bonne nouvelle. Car si l'identité de l'ampoule se retrouve compromise, les pirates ont alors la possibilité d'avoir accès à des informations sensibles comme le mot de passe de votre réseau Wi-Fi et ainsi à tous les appareils qui y sont reliés. De cette façon, l'ampoule servira de relais pour passer d'un réseau à un autre. Les autres vulnérabilités rendant beaucoup trop facile le décryptage de ce matériel intelligent seraient en partie dues à la fragilité du code de vérification établi dans la Tapo L530E ainsi que le manque de caractère aléatoire dans le chiffrement de l'ampoule connecté.

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

On pourrait se croire dans un film d'espionnage, mais c'est bel et bien vrai : nous pouvons tous nous faire pirater par ampoule connectée. L'entreprise TP-Link productrice des ampoules précédemment énoncées aurait d'ailleurs affirmé lancer prochainement une mise à jour du programme informatique faisant fonctionner certaines de ses ampoules, mais, sans pour autant préciser quelles versions devraient rester vulnérables au hackage. Encore trop peu sécurisées par leurs concepteurs, la domotique en général inquiète les plus grandes instances internationales. La Commission européenne a proposé en 2022 de mettre en place une loi nommée Cyber Resilience Act obligeant aux fabricants d'appareils intelligents de prendre en compte la sécurité de l'objet connecté dès sa conception, tout au long de son cycle de vie ou du moins durant cinq ans ainsi. qu'à obliger les industriels à signaler les vulnérabilités et les incidents exploités de façon claire et compréhensible aux utilisateurs. Mais pour l'instant, la meilleure façon de se protéger face à ce type d'attaque reste de régulièrement mettre à jour les logiciels de vos appareils intelligents, d'utiliser un mot de passe résistant, difficil à déchiffrer et de modifier celui par défaut de votre routeur, d'activer la double authentification de votre matériel électronique ainsi que de configurer un réseau Wi-Fi distinct pour vos appareils connectés.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, pensez à vous abonner dès à présent à ce podcast, vous pouvez le faire sur plusieurs applis audio comme Amazon Music par exemple et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous invite à découvrir notre dernier épisode de Bête de Science dans lequel Gaby Fabresse vous dévoile les facultés peu connues d'un animal qui nous côtoie pourtant depuis des millénaires, j'ai nommé la vache. 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.*]