

## Les pacemakers dans le collimateur des pirates informatiques

VIDÉO. Les stimulateurs cardiaques cibles des hackers ? Une équipe de chercheurs lillois l'envisage sérieusement. De quoi se faire très peur.

Par Baudouin Eschapasse

Publié le 02/02/2016 à 12h48, mis à jour le 02/02/2016 à 17h23



C'est un scénario digne d'un film d'horreur. Le cabinet de conseil en stratégie numérique Suricate Concept affirme qu'il est aujourd'hui possible de tuer des milliers de personnes... d'un simple clic ! Comment ? Tout simplement en s'en prenant aux pacemakers qui équipent 5 millions d'individus de par le monde.

En **France**, un peu moins de 400 000 individus sont porteurs de stimulateurs cardiaques. Un chiffre en progression constante depuis 20 ans. 60 000 patients se font poser chaque année ces appareils de la taille d'un sachet de thé qui envoient de petites impulsions électriques pour corriger des dysfonctionnements du cœur : soit qu'il ne batte pas assez vite, soit que ses ventricules ne soient pas bien synchronisés.

Or, les pacemakers sont des « objets connectés ». Cette connexion se faisait par onde radio depuis les années 1970. Elle se double aujourd'hui

d'un système Bluetooth pour les défibrillateurs portables de « dernière génération » .

## Des objets connectés insuffisamment protégés

« Lorsque les fabricants de stimulateurs cardiaques nous ont expliqué que leurs machines étaient connectées, on s'est dit qu'on avait un sérieux problème », explique Monir Morouche, président de l'agence Suricate Concept qui avait déjà fait parler de lui, l'an dernier, en démontrant combien il est facile de « pirater » un téléphone portable.

« Les objets connectés sont en effet particulièrement exposés aux **tentatives d'intrusion de tiers** », déclare ce jeune chercheur en informatique de 27 ans, « totalement autodidacte ». À l'en croire, il serait terriblement simple pour des « pirates » d'en prendre le contrôle. Chef de bande d'une poignée de petits génies du cybermonde, il a exploré les failles de ces équipements et développé les lignes de code susceptibles de « manipuler à distance » ces engins minuscules. « Nous n'avons mis que quatre mois pour y parvenir », émet-il.

Que les pacemakers soient ainsi exposés à des attaques informatiques, cela fait plusieurs années que les chercheurs le savaient. Le Néo-Zélandais, Barnaby Jack avait déjà pointé du doigt de graves failles de sécurité en 2013. Il était d'ailleurs sur le point de faire une démonstration grandeur nature de l'ampleur du problème lorsqu'il est décédé dans des conditions mystérieuses. C'est cependant la première fois qu'un programme est mis au point pour détraquer leur fonctionnement, assurent les membres de Suricate.

## De quoi se faire très peur

Pour attirer l'attention des médias, cette agence de consulting a réalisé une bande-annonce aux faux airs de film catastrophe américain. La start-up a par ailleurs communiqué sa « découverte » en marge du **8e Forum international de la cybersécurité (FIC)**. À l'en croire, des virus informatiques relativement simples permettraient de perturber profondément (et durablement) le fonctionnement de ces matériels de santé d'importance vitale en jouant sur les micro-contôleurs des pacemakers.

Il serait ainsi très facile d'augmenter artificiellement le rythme cardiaque d'une personne. Confronté à une augmentation de la température corporelle relevée par ses capteurs, un stimulateur cardiaque en déduit

que son porteur est en train d'effectuer un effort physique et augmente la pulsation. « Nous sommes en mesure de simuler une poussée de fièvre et donc de pousser le muscle cardiaque au-delà de ses limites de résistance », assure Monir Morouche. Mais ce mode d'action est loin d'être le seul possible.

## Le crime parfait

Au sein d'un projet, judicieusement baptisé « hacking dead », le jeune homme, appuyé par quatre ingénieurs informatiques (Dylan Lespagnol, Mehdi Bendjebara, Farouk Jebali et **Jacques-Olivier** Lis), a imaginé d'autres types d'attaques possibles. « En faisant s'emballer un pacemaker, il est facile de faire exploser sa pile au lithium », affirme ainsi Monir Morouche. « Si le coeur du patient survit au choc initial, le liquide de la batterie qui se répandra dans son corps devrait l'achever de manière imparable », poursuit le jeune homme.

Il affirme que son équipe serait parvenue à mettre au point un virus qui, une fois inoculé dans le pacemaker d'un individu, pourrait être propagé à la faveur de ses déplacements. Via Bluetooth. Transmis à d'autres porteurs de pacemakers, il pourrait, toujours selon lui, infecter les serveurs des structures hospitalières qu'il fréquente. « Aucun portique de sécurité ne peut le détecter », souligne M. Morouche.

Pire ! Ce virus informatique pourrait être téléchargé à l'insu de son porteur à partir de n'importe quel objet domotique connecté. « Nous avons fait un essai depuis un réfrigérateur. Cela fonctionne », complète l'un de ses comparses.

## Un enjeu de sécurité

Monir Morouche affirme avoir transmis le code source capable de provoquer un tel accident aux autorités compétentes pour que la faille technique soit vite corrigée. « Nous sommes des lanceurs d'alerte, pas des irresponsables », avance l'expert informatique qui se dit, par ailleurs, en contact avec le directeur technique du FBI, mais aussi le responsable de la sécurité des systèmes d'informations du ministère des Affaires sociales.

Faut-il s'inquiéter de ces révélations quand on sait que Daech **réfléchit à des cyber-attentats** ? Les spécialistes en cybersécurité se veulent rassurants. « Les pirates informatiques ciblent prioritairement les secteurs où ils peuvent faire de l'argent, ce qui n'est pas le cas ici. Les terroristes

n'ont par ailleurs pas encore la capacité technique de commettre de telles attaques », déclare Jérôme Robert, directeur marketing de Lexsi, société spécialisée dans la cybersécurité. « Nous mettons tout en oeuvre pour assurer la sécurisation des outils numériques touchant à la santé humaine », complète, de son côté, Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information.

En attendant, des producteurs de cinéma ont contacté l'agence Suricate Concept pour développer un film autour de leur « invention ». On aimerait tant que leurs anticipations restent du domaine de la science-fiction !