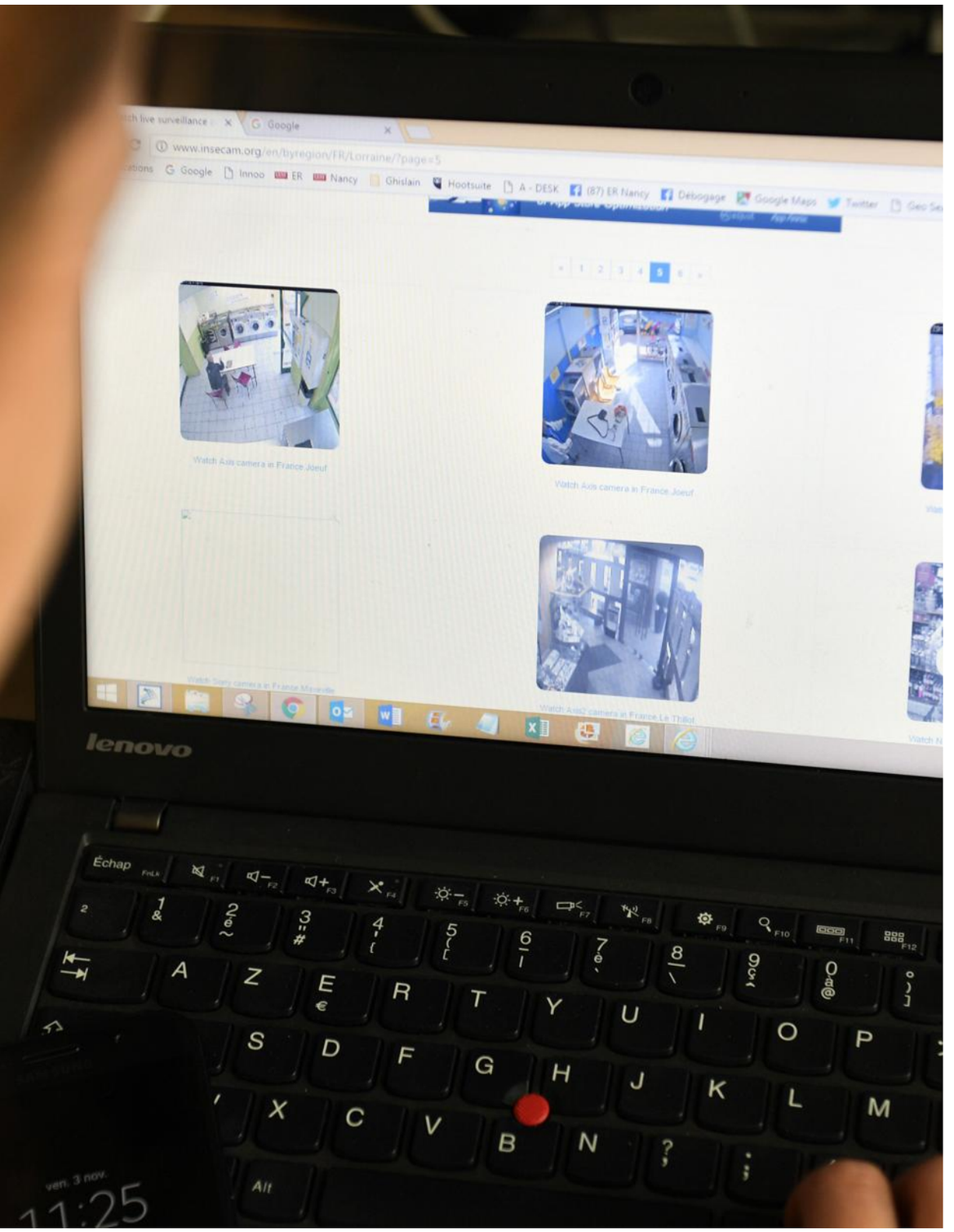

Des milliers de caméras sont accessibles sur le site insecam.org. La Meurthe-et-Moselle n'échappe pas à sa fuite d'images. Photo Pierre MATHIS

« Prendre le contrôle d'une webcam est un jeu d'enfant »

Toute l'équipe de Cyber Detect, la start-up nancéienne qui développe l'antivirus le plus puissant du monde. D.R

Adossé au Laboratoire de haute sécurité du Loria (Laboratoire lorrain de recherche en informatique et ses applications Inria, CNRS UL), Cyber-Detect est une spin-off spécialisée dans la sécurité informatique. Selon Laurent Werner, président de cette start-up nancéienne qui développe une nouvelle génération d'antivirus, prendre le contrôle d'une webcam ou de tout autre objet connecté est un jeu d'enfant. « Tous les objets connectés ne font qu'émettre et recevoir des informations. Leur firmware, le logiciel qui les gère, n'est pas assez important pour accueillir un anti-virus ». Les hackers n'ont donc aucun mal a constitué un ou des « botnet » (des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches) qui prend la main sur un maximum de webcams.

« L'objectif est de faire du buzz. Leur action n'est pas malveillante. C'est presque de la cybersécurité puisqu'ils pointent du doigt les failles d'un système. C'est une façon de montrer qu'ils sont capables de voir ce que personne ne perçoit. Ils montent un site pour le faire savoir. Ça attire les voyeurs, ça crée de l'audience et ça génère des revenus publicitaires. »

Comment s'en prémunir ? Il y a un moyen très simple : changer de mot de passe. Souvent les IOT sont vulnérables parce qu'ils ont encore le mot de passe constructeur du style « admin ». Pour autant, un bon hacker pourra faire sauter un mot de passe. Les industries sont équipées de système de vérification d'intégrité qui attaque les « bouts de code » en trop qu'on aurait pu installer de manière furtive sur les objets connectés.

Propos recueillis par
Saïd LABIDI