Boeuf séché, hoverboards et hackeur·euse·s

Par Misch Pautsch

Publié le 15 oct. 2021

Changer en allemand pour l'article original

Comment prendre contact avec un groupe de hacker·euse·s? Par email, apparemment. Ils répondent rapidement, ce qui n'est pas vraiment surprenant. Mais on peut aussi visiter le siège officiel de leur asbl à Luxembourg-ville : la «Chaosstuff». Une conversation avec des bricoleur·euse·s qui défient la définition classique du «hacker».

Le nom du Chaos Computer Club est généralement mentionné dans les médias lorsque quelque chose va mal. Au Luxembourg, cela a été le cas récemment lors de la fuite de données sur le nouveau site web pour les pétitions en ligne. Mais on pense aussi à l'affaire de la fuite de la Chambre en 2018, et à la fuite sur l'application de campagne électorale de la CDU en Allemagne en mai 2021, qui se sont toutes deux soldées par des actions en justice – aujourd'hui retirées. Dans les deux cas, les Chaos Computer Clubs luxembourgeois et allemand ont chacun vivement critiqué les actions en justice engagées contre les lanceurs d'alerte et ont plaidé pour que les responsables des sites prennent également leurs responsabilités au lieu de s'en prendre aux messagers.

« Ces moments sont probablement ceux pour lesquels la plupart des gens nous connaissent », confirme Dennis Fink du Chaos Computer Club Luxembourg (C3L) : « Et c'est certainement une grande partie de notre travail, peut-être la plus importante, que d'éduquer les gens sur la technologie, la digitalisation, les droits d'auteur et la protection des données. » Cependant, lorsque le nom d'un groupe n'apparaît presque toujours que dans le contexte de mauvaises nouvelles, ce goût amer risque parfois de déteindre sur les personnes concernées. Le fait que le terme « hackeur·euse » soit culturellement lourd n'aide pas. Selon les circonstances, il est associé à quelque chose qui va de l'espièglerie à la criminalité pure et simple.

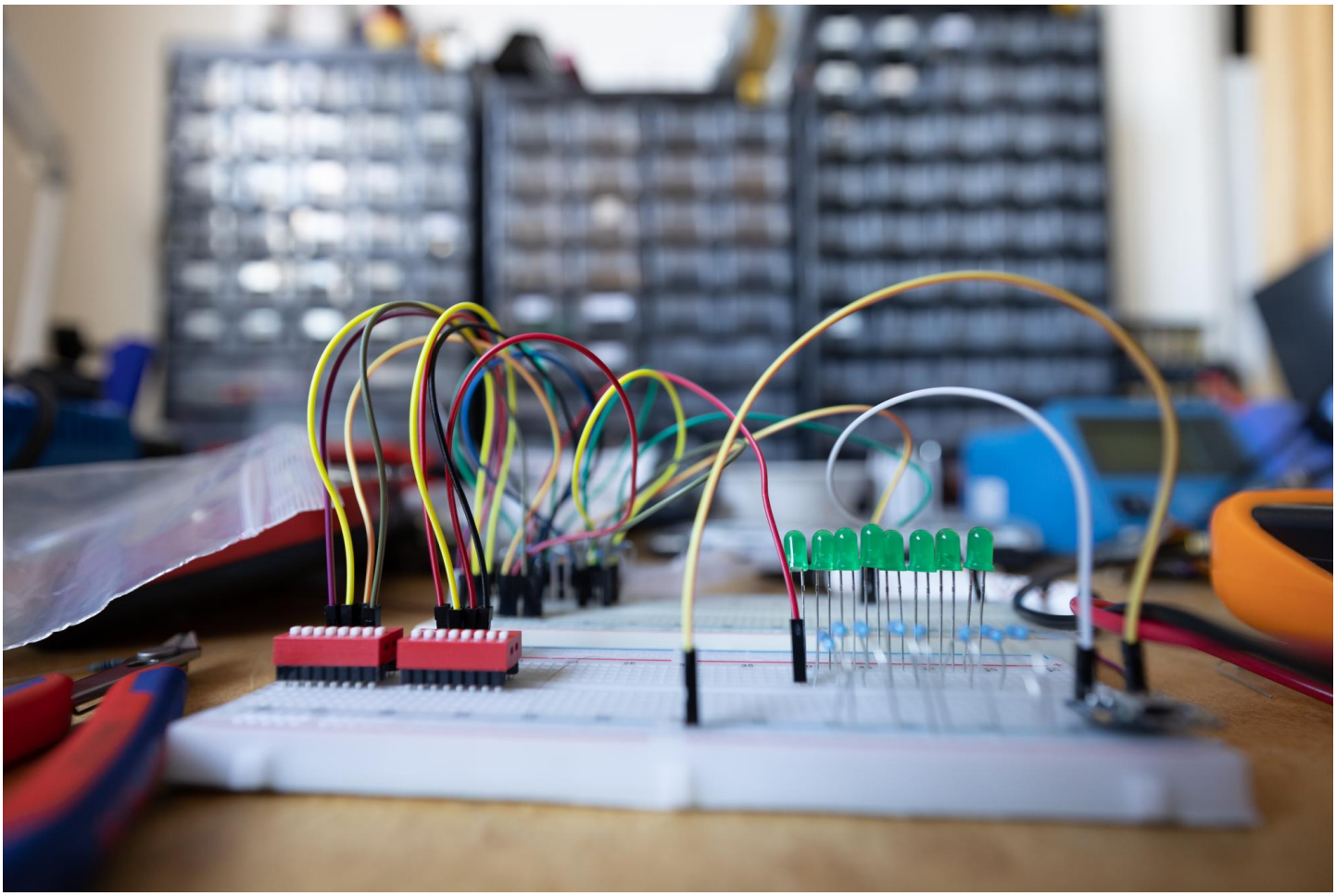
Dennis Fink

« Chaque fois que la presse parle d'une attaque informatique, déplore Dennis Fink, elle parle de ce que nous appelons des « crackers ». C'est-à-dire des personnes ou des groupes qui tirent un avantage personnel d'attaques souvent criminelles. Les « Blackhats », comme beaucoup les appellent. » Il s'agit d'une référence aux films westerns classiques, dans lesquels les méchants portaient généralement des chapeaux de cow-boy noirs et les héros des chapeaux blancs. « Maintenant, nous ne sommes pas tout à fait des « whitehats » – ces professionnels de l'informatique qui travaillent pour des sociétés de sécurité ou l'État, par exemple – mais plutôt des « greyhats », c'est-à-dire que nous avons une attitude critique envers l'État, tout en défendant les droits des gens. »

Reconstruction

Les relations publiques sont certainement la partie la plus importante de l'association, mais ce n'est qu'un des nombreux éléments qui font moins la une des journaux. Les membres de C3L sont des « hackeur·euse·s » au sens classique du terme : ce sont des bricoleur·euse·s. Les premiers hackeur·euse·s autoproclamé·e·s étaient des étudiant·e·s du Tech Model Railroad Club du MIT (Massachusetts Institute of Technology). Le nom n'est pas une couverture astucieuse pour cacher des actions

louches dans une salle de club. Non, il s'agissait d'un groupe de passionné·e·s de chemins de fer miniatures qui ont progressivement élargi leur hobby grâce à des « hacks », des solutions techniques aux difficultés qu'ils rencontraient en bricolant.



Le C3L, comme tous les clubs informatiques du Chaos, poursuit cette tradition. Si vous utilisez une technologie à des fins autres que celles pour lesquelles elle a été conçue, vous « hackez ». « En ce sens, nous sommes définitivement des hackers. Le meilleur exemple est un déshumidificateur dans notre studio qui est destiné à la fabrication de bœuf séché. Nous l'utilisons pour garder au sec le matériel dont nous avons besoin pour l'imprimante 3D. Il réagissait à une forte humidité, il nous fallait donc une solution. Un hack. »

Tout comme dans le Tech Model Railroad Club, qui a progressivement évolué vers l'informatique pour automatiser davantage ses propres modèles, dans C3L tout le monde peut parler de ses intérêts. « Cela va de la question de savoir comment cultiver au mieux des piments – c'était un projet plus vaste – à un skateboard que nous avons converti avec les pièces d'un hoverboard afin de pouvoir le contrôler à distance, en passant par les discussions les plus ringardes sur les paramètres des algorithmes de

cryptage », explique M. Fink. Pour beaucoup, cependant, la question de la sécurité informatique et de la protection des données est au cœur de C3L.

« Par-dessus tout, outre l'éthique du hackeur, il y a une « règle » : être excellent les uns envers les autres. Notre objectif commun est d'aider la société, de défendre la liberté d'information et de protéger les données privées. » Selon Dennis Fink, un moment clé de la coopération avec les acteurs publics a été deux vidéoconférences avec des partis politiques, au cours desquelles le groupe a pu faire part de son opinion sur la réforme prévue du droit d'auteur. « Plusieurs députés ont déjà posé des questions parlementaires en réponse à nos communiqués de presse auparavant, mais nous espérons bien sûr que cette évolution vers le dialogue se poursuivra. En ce qui concerne la réforme du droit d'auteur, par exemple, il semble pour l'instant, pour autant que je sache, que notre retour d'information n'ait donné lieu à aucun changement. À mon avis, beaucoup de sections n'ont pas été conçues avec beaucoup d'intelligence . »

« Vous ne donneriez pas votre carte de crédit à un étranger, après tout. »

Dennis Fink, C3L

Une autre évolution que C3L observe d'un œil critique est le développement rapide de la collecte et de la reconnaissance des données biométriques. Au niveau de l'UE, l'interdiction des technologies permettant d'identifier les personnes par leur démarche, leur posture, leur comportement de frappe ou la reconnaissance faciale, entre autres, est discutée depuis un certain temps. Toutefois, une décision finale sur les mesures à prendre n'a pas encore été prise. « Nous voyons la tendance selon laquelle de tels systèmes peuvent être et seront également intégrés dans les caméras de surveillance. Il sera possible de reconnaître encore mieux les profils de mouvement, et dans deux ou trois ans, il sera probablement possible d'enregistrer les émotions. En même temps, nous voyons que les caméras sont placardées partout ici aussi... »

En réseau

L'éternel argument selon lequel ceux qui ne font rien de mal n'ont rien à craindre n'est pas accepté par Dennis Fink avec un sourire. Parce que les défenseur·euse·s de la protection des données ont trop souvent entendu la même vieille histoire, ils ont une réponse toute prête : « Vous fermez aussi la porte des toilettes quand vous allez aux toilettes chez vous. Bien sûr, c'est un peu désinvolte, donc en autres mots : vous ne donneriez pas votre carte de crédit à un inconnu. » Disposer de données sur les gens donne du pouvoir ; ce n'est pas pour rien que le marché du comportement des consommateurs est devenu l'un des domaines les plus importants du commerce, notamment depuis la pénétration des médias sociaux dans toutes les étapes de la vie : C'est l'affaire de Facebook et de Google, les titans de la révolution numérique. Et de plus en plus un outil de contrôle social.

« Pourquoi un État devrait-il être autorisé à faire ce que les autres ne font pas ? », demande M. Fink. « Beaucoup de gens ne se rendent pas compte de ce que la vie privée nous apporte chaque jour, à nous et à l'humanité tout entière. Elle nous permet de nous épanouir, d'être qui nous sommes. Prenez la dépression, par exemple. Tout le monde n'a pas besoin de savoir qu'une personne souffre d'un problème de santé mentale. Ni l'État, ni l'assurance maladie ». Que les coûts des assurances, par exemple,

augmentent « parce que tout le monde sait tout sur vous, nous pensons que ce n'est pas nécessaire. »

Même ceux qui font aveuglément confiance aux grands collecteurs de données, gouvernementaux ou privés, feraient bien d'espérer que leurs informations ne tombent pas entre de mauvaises mains. Comme, par exemple, lors d'une série d'attaques de ransomware contre des hôpitaux aux États-Unis. Les pirates ont bloqué leurs systèmes informatiques, parfois pendant plusieurs jours, ce qui a non seulement retardé le traitement de nombreux patients, mais aussi, selon les porte-parole des

hôpitaux concernés, augmenté considérablement le taux de mortalité pendant cette période.

Les enquêteurs soupçonnent des gangs russes bénéficiant du soutien de l'État d'être à l'origine de cette attaque, qui ne devait pas être la seule : Des attaques similaires ont paralysé un pipeline de Colonial le 7 mai 2021, puis un peu plus tard le 1er juin JBS, le plus grand transformateur de produits carnés des États-Unis.

Un clic?

« Savez-vous que tous les compteurs d'électricité du Luxembourg et de la plupart des pays européens sont connectés à internet ? Les “compteurs intelligents” ou “Smartmeter”. » Dennis Fink lève les sourcils. « Ils sont super cool, bien sûr. Vous pouvez mesurer combien vous consommez et quand, ils peuvent être intégrés dans des réseaux intelligents qui rendent le réseau électrique plus stable. Seulement, malheureusement, ils ont un piège. L'opérateur peut simplement les éteindre à distance », claque-t-il des doigts. « Il ne fait pas ça normalement, bien sûr. Mais comme ils sont connectés à internet, l'internet est également connecté à eux. Il suffit qu'une seule personne trouve une faille de sécurité pour couper l'électricité de tout le Luxembourg si l'envie lui en prend », explique le C3L.

« Pourquoi ces réseaux ne peuvent-ils pas être reliés à l'internet ? Même dans les hôpitaux. Pourquoi ces ordinateurs doivent-ils tous être connectés à Internet ? Pour certaines infrastructures, bien sûr que c'est nécessaire, mais toujours pour toutes ? Pourquoi ne pas créer un intranet ? Ou, comme nous le disons parfois en plaisantant ici, un « Luxembourg-net » ? Bien sûr, cela coûterait plus cher, mais mieux vaut cela que de vivre avec la crainte qu'une seule personne puisse saboter le réseau électrique dans toute l'Europe. »

Le concept d'économie des données est au cœur de la sécurité informatique et, selon Dennis Fink, il devrait également être davantage exigé. L'une des questions centrales dans les fuites de la Chambre était de savoir pourquoi les données sensibles se trouvaient sur un serveur accessible au public en premier lieu, dit M. Fink : « Sur un serveur qui est connecté à Internet, seules les données qui sont nécessaires devraient s'y trouver. » Une fois que quelque chose est sur Internet, on ne l'oublie pas. « C'est pourquoi nous voyons chacune de ces situations comme une petite bataille, où nous essayons de contrecarrer les décisions qui nous semblent problématiques. Il y a des batailles qu'on gagne, d'autres qu'on perd. »

Tant que des intérêts particuliers tenteront de restreindre la vie privée, de maintenir ouvertes des portes dérobées et d'imposer aux internautes des technologies potentiellement dangereuses, les hackeur·euse·s garderont un œil sur l'évolution de la situation. Et entre deux discussions sur la meilleure façon d'arroser les piments.