Shutterstock - Nazarkru

JULIEN JOLY
& ROMAIN ROUX
rennes@lemensuel.com

HACKERS ÉTHIQUES DE RENNES
LES ROBINS DU WEB

Le hacker, ce spécialiste de la sécurité informatique, est souvent vu comme un malveillant pirate du web. Certains mettent pourtant leurs talents au service de la bonne cause. Véritables cyber-justiciers, ces « hackers étiques » sont nombreux à Rennes.

Quand on parle de hackers, on imagine volontiers des ados blafards en sweat-shirt à capuche, capables de pirater une banque en trois clics depuis la pénombre de leur chambre. La réalité est plus terre à terre. Chercheurs d'université, employés de bureau, pères ou mères de famille, les hackers sont avant tout des curieux passionnés de cybersécurité.

Oui, certains sont animés de mauvaises intentions. Leur ombre plane sur l'attaque massive de sites gouvernementaux ukrainiens, en janvier, dans un contexte de tensions avec la Russie. Ou sur le chantage au rançongiciel qui a frappé le français LDLC en novembre dernier.

A contrario du « méchant hacker » sans foi ni loi (surnommé « black hat » dans le jargon), il existe aussi des « hackers éthiques » (ou « white hats »). Ces derniers, qui revendiquent un code de conduite exemplaire, colmatent les failles de sécurité, aident des militants à rester sous le radar des dictatures ou dissèquent les nouveaux virus informatiques. Pour les trouver, pas besoin de fouiller les profondeurs du web. Arpentez plutôt les couloirs de Rennes 1 ou des entreprises locales spécialisées dans la protection numérique.

« Le hack légal est le choix de la raison, celui qui m'aide à dormir la nuit », témoigne Adrien Jeanneau. Ce Rennais participe à des bug bounties, des programmes rémunérés mis en place par des sociétés pour récompenser qui détectera une brèche dans leur système. Adrien a notamment traqué les défauts de l'application gouvernementale StopCovid. Aujourd'hui, il travaille chez YesWeHack, une importante plateforme de bug bounty basée en région rennaise.

La capitale bretonne, autrefois fief des télécoms, est devenue une place forte de la cybersécurité tricolore. On y trouve une antenne du commandement de la Cyberdéfense française. En 2023, l'Agence nationale de la sécurité des systèmes d'information (Anssi) plantera son drapeau à La Courrouze. Cet écosystème foisonnant représente 4 242 emplois civils et militaires, si on compte les 96 entreprises privées du secteur, comme Amossys, où travaille l'auditeur Karim Chahal. « Rennes devient une ville importante pour le cyber, confirme-t-il, alors qu'on n'en parlait peu il y a cinq ans. C'est un sujet qui concerne tout le monde. » Et pour cause. Selon une étude d'Orange cyberdefense, dont Rennes est le fer-de-lance, le nombre de cyberattaques contre les entreprises a augmenté de 13% en un an. ●

CHANTAGE À LA SEXTAPE
IL FAUT TOUJOURS AVOIR UN HACKER DANS SA POCHE

Quelque chose cloche dans le message reçu par Laure, en novembre dernier. Cette mère de famille rennaise va vite en avoir le cœur net. Un pirate vient de prendre le contrôle du compte Facebook de son compagnon. Dans la conversation entre les deux amants, le hacker a trouvé de quoi de les faire chanter : des photos et vidéos intimes. « J'ai toujours fait attention à ce qu'on ne voie pas ma tête et mon corps en même temps, souligne la quadragénaire. Mais c'est facile de me rendre reconnaissable, j'ai des signes extérieurs distinctifs. » Si elle ne veut pas que sa vie soit déballée à ses proches et son employeur, elle doit payer.

La mère de famille garde la tête froide. Et comprend qu'elle a un avantage : l'escroc perdrait son moyen de pression en mettant, tout de suite, sa menace à exécution. Il faut donc le faire attendre et le laisser espérer, le temps de trouver une solution. Coup de chance, un ami rencontré par hasard ce jour-là lui glisse un nom. Il y aura en fait deux sauveurs : Thomas, conseiller en économie et stratégie numériques, et son collègue Lucas, spécialisé dans la cybersécurité. Ce n'est pas la première fois qu'ils filent un coup de main à des connaissances.

Jeu d'enfant

Le premier comprend vite le tableau. « Le compagnon de Laure a dû se connecter à un wifi public, comme ceux des bibliothèques ou des cafétérias. » À distance, le hacker s'est sans doute introduit sur le réseau pour aspirer les données des utilisateurs, notamment leurs identifiants et mots de passe. Avec ces informations, facile de se connecter à la boîte mail de la victime. Et si le code d'accès est le même sur Facebook, usurper le compte est un jeu d'enfant. Il n'a plus qu'à changer tous les mots de passe pour rendre impossible la connexion du vrai propriétaire.

Lucas prépare alors le coup d'après. Le but : prendre l'attaquant à son propre jeu. Lui demander un Rib pour verser l'argent, une adresse mail, un numéro de téléphone… Lucas espère pouvoir ainsi « hameçonner » le hacker. Un peu comme notre grand-mère qui transmet son code de carte bleue après avoir cliqué sur un lien frauduleux. Mais en un peu plus sophistiqué. « L'objectif est de le pousser à la faute pour récupérer des informations sur lui et retourner le chantage. »

Heureusement, la stratégie n'a pas besoin d'être exécutée. Sur les directives des deux spécialistes, Laure prend contact avec Facebook pour demander la suppression du compte piraté de son compagnon. La firme américaine ne le fait qu'au bout de dix jours. Une semaine et demie pendant laquelle la Rennaise doit relancer et prouver l'usurpation, sans personne à qui parler du côté de l'entreprise car tout se passe en ligne. « Lors d'un piratage, l'accès à un support efficace auprès d'une plateforme est souvent difficile à cause du nombre de cas à traiter, déplore Lucas. C'est pour ça qu'il faut se focaliser sur les causes, en formant les utilisateurs. »

LE BUT : PRENDRE L'ATTAQUANT À SON PROPRE JEU

La mère de famille s'en est sortie grâce aux précieux conseils de deux « Robins du web ».

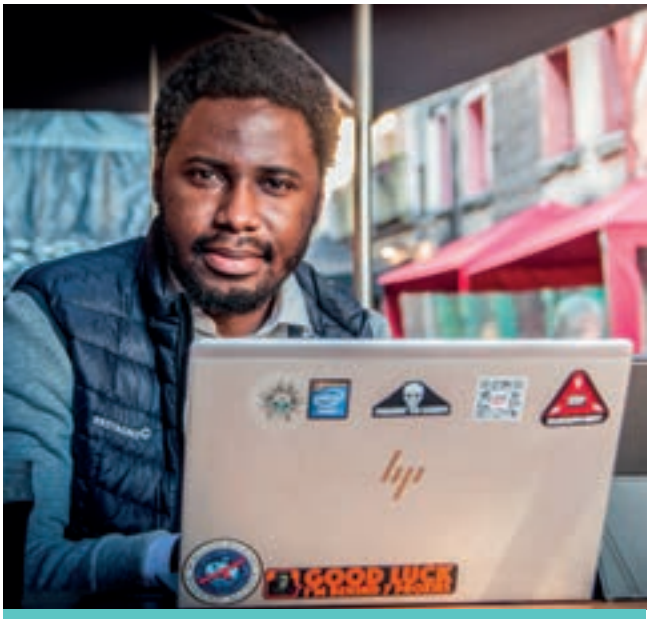
Laure aimerait pouvoir dire que l'histoire se termine bien. Après tout, elle n'a pas payé. Mais rien ne dit que le hacker s'est débarrassé des images et des données volées. Il pourrait les vendre à un site ou à d'autres pirates. « J'ai toujours ce petit truc qui me dit que je ne suis pas totalement maître de mon destin. » ●

1. Le prénom a été modifié.

Pxhere

SAXX LA DÉVOTION DU SACRÉ HACKER

Assis à la terrasse d'un hôtel de luxe dont il refuse de donner le nom, son ordi portable ouvert devant lui, Clément Domingo hésite. Le chercheur rennais en cybersécurité doit absolument récupérer une information sur Internet. Mais le seul moyen d'y accéder est le wifi public de l'établissement. Une passoire numérique, le meilleur moyen de se faire siphonner ses données en moins de deux. Tant pis. Il s'y risque. Mais quelque chose cloche dans l'interface de connexion. Intrigué, le trentenaire « trifouille » numériquement quelques secondes. Et le voilà qui tombe dans une zone interdite : le logiciel d'administration de l'hôtel. Sous ses yeux défilent les listings des clients, la vidéosurveillance… Un pirate informatique en aurait profité pour barboter de précieuses informations. Clément Domingo, lui, se déconnecte et avertit l'hôtel de cette grave faille de sécurité. Quand il rapporte l'incident sur son blog, c'est expurgé de tout indice qui aurait permis de réitérer l'exploit. Le jeune Rennais est ce qu'on appelle un hacker éthique. Ça implique une certaine discrétion professionnelle. Il finit souvent ses phrases par un mystérieux « je ne peux pas en dire plus ».



Clément Domingo, alias SaxX, vient en aide aux entreprises victimes de cyberattaques.

Sous son pseudo, SaxX, il vient en aide (moyennant finances) à des entreprises victimes de cyberattaques. Ce qui peut survenir n'importe quand et nécessite une attention immédiate. Lors de notre premier rendez-vous dans un café, son téléphone sonne et il rebrousse chemin brusquement : « Urgence opérationnelle. Je dois me mettre au boulot. Je ne vais sans doute pas dormir pendant les prochaines 24 h. » L'intégrité informatique d'un client est menacée. Lequel ? « Oublie ça, c'est sensible. » Vivre sur la brèche, Clément adore. Ses phrases prennent souvent des virages à 90° au gré de ses idées. Il bouillonne. Multiplie les projets. Quand il ne hacke pas, il se fait DJ dans les bars, ou apprend la serrurerie. Afin de démocratiser la cybersécurité, il coorganise la BreizhCTF, une compétition de hackers dont la 7e édition aura lieu le 1er avril à Rennes. Il vient de cofonder l'ONG Hackers sans frontières. « C'est énorme. J'ai pas dormi depuis 28 h ! »

Le pire, c'est qu'il a encore le temps d'intervenir bénévolement en milieu scolaire. « Les jeunes n'ont pas les codes. Ils utilisent tous Tiktok ou Snapchat mais ne savent pas comment ça fonctionne. Ensemble, on parle de cyberharcèlement. Je leur apprends à faire des mots de passe sécurisés. Ils me disent : "J'ai rien à cacher." C'est faux. Avec juste un pseudo ou un "like", on peut retrouver quelqu'un. »

IL A COFONDÉ L'ONG HACKERS SANS FRONTIÈRES

En vacances, il ne tient pas en place, taquine la sécurité des forfaits de ski avec une sorte de télécommande high-tech. « Ça identifie tout ce qui est sans contact. Une fois, j'ai découvert qu'on pouvait obtenir des boissons à l'infini en bidouillant la carte de recharge d'un bar. Bien sûr, j'ai prévenu le patron. » On n'en attendait pas moins de ce paroissien de Saint-Germain, ancien responsable d'un chapitre au pèlerinage de Chartres. Encore une casquette inattendue… ●

J. Joly

SÉCURITÉ OFFENSIVE
MANIPULATEURS ET SANS REPROCHES

Les Pères Noël avaient bien préparé leur coup. « Ils sont entrés dans les bureaux avec des manteaux rouges, un sapin et des guirlandes. Le personnel était content, tout le monde croyait à une animation. Sauf qu'en installant le sapin à l'accueil, ils en ont profité pour poser des implants dans le faux plafond. » De quoi infiltrer à distance le réseau de la boîte. Joli cadeau !

Les hackers peuvent laisser traîner des clés USB infectées, ou cloner un badge d'accès depuis une poche.

L'incident, survenu l'année dernière, est raconté par Yann Cam. Ce spécialiste de la cybersécurité chez Synetis, à Rennes, n'a pas participé à l'opération. Mais il en connaît les orfèvres, des hackers coutumiers de ce type d'attaque « physique ». Heureusement, il ne s'agissait là que d'un test, commandé par une entreprise pour mesurer sa vulnérabilité face à une stratégie inattendue. Car les hackers ne passent pas tous leur journée devant un écran d'ordinateur. Et la faille qui leur donnera les clés de vos données est souvent un employé trop confiant.

Yann fait partie de ces professionnels capables de monter des scénarii dignes de la série d'espionnage *Le Bureau des légendes* pour s'approcher au plus près d'une cible. Il ressemble d'ailleurs un peu à un personnage de télé, avec son foulard, sa petite barbe, ses cheveux courts et ses yeux clairs. « Le monde de la cybersécurité m'a passionné dès le collège. Mais à l'époque, il n'y avait pas de formation apprenant à pirater pour mieux sécuriser. » Moins connues que les attaques informatiques classiques « qu'on peut faire en robe de chambre depuis son canapé », les « intrusions physiques » se démocratisent en France. Pourquoi pirater des ordinateurs à distance si on peut crocheter la serrure de la salle des serveurs ?

Quand Yann endosse le rôle d'un attaquant malveillant, c'est toujours avec l'assentiment du client, dans le cadre d'un audit de sécurité très cadré. « On demande, par exemple, si on peut tenter de manipuler les employés, envoyer un drone pour mieux capter la wifi, ou utiliser une pince-monseigneur. Ça surprend les gens. Mais notre métier est aussi de les sensibiliser. »

Parmi ses techniques, « le test du faux stagiaire ». « On arrive innocemment dans les locaux comme si on avait été embauché, on se branche sur une prise RJ45 et on voit tout ce qu'on est capable de dérober. On peut aussi laisser traîner des clés USB infectées dans les toilettes, cloner un badge d'accès depuis une poche… » Débarquer avec un gilet fluo d'électricien donne accès à plein de cloisons derrière lesquelles poser un mouchard. Moins rigolo qu'un costume de Père Noël, mais moins suspect.

Et personne n'est à l'abri. « Lors d'une attaque sur un grand groupe espagnol, on a déduit le mot de passe d'un employé haut placé. On l'utilise pour se connecter. Sauf que le système envoie une demande de confirmation sur son portable. » Vite, un plan B ! « On appelle l'employé en espagnol, en se faisant passer pour le support informatique : "Vous êtes en télétravail ? Votre ordinateur est lent, non ? Vous devez télécharger un nouveau VPN…" » À son insu, la victime installe un programme à la solde des hackers.

ENVOYER UN DRONE SUR LE BÂTIMENT POUR MIEUX CAPTER LA WIFI

Faire l'espion sans risquer la prison, un métier de rêve ? « Oui, c'est tout à fait sympathique », sourit Yann. Aux jeunes qui voudraient se lancer, il conseille : « Maîtrisez la programmation, les systèmes d'exploitation et les réseaux. Apprenez à exploiter des brèches sur des plateformes de challenge comme Hack the box ou Root-me. Ne piratez jamais une cible sans son accord ! C'est une question d'éthique. » ●

J. Joly

DONNÉES PERSONNELLES
VOTRE VIE PRIVÉE, ÇA LES REGARDE

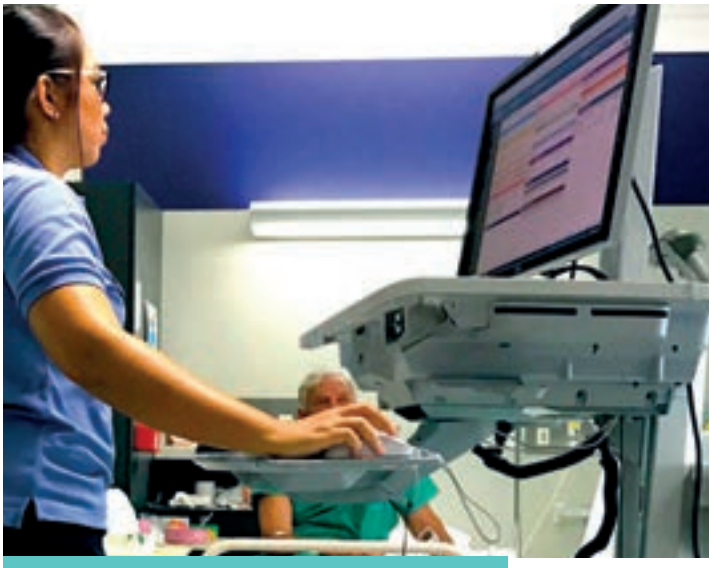
1,4 million : c'est le nombre de personnes victimes d'un vol massif de données de santé à l'Assistance publique-Hôpitaux de Paris, l'été dernier. Les pirates avaient ciblé un fichier lié aux dépistages de la Covid-19. Cette attaque fait partie des nombreux raids informatiques menés contre des structures de santé depuis le début de la pandémie. Elle vient nous rappeler à quel point notre vie est désormais intriquée avec le virtuel.

> « EN FRANCE, LE NIVEAU DE CYBERSÉCURITÉ N'EST PAS ÉMINEMMENT ÉLEVÉ »
>
> **ANTHONY BOUVET,**
> *pentester*

Doctolib, Whatsapp, Deliveroo… Autant d'applications utilisées quotidiennement et à qui nous confions aveuglément nos adresses, coordonnées bancaires ou soucis de santé. Ces informations valent très cher. Une base d'e-mails et de mots de passe, achetée sur des forums spécialisés, permet de lancer de manière automatique des milliers de tentatives de hameçonnage. D'autres n'hésitent pas à subtiliser les données d'une clinique contre rançon, mettant en jeu la vie des patients.

Parfois, c'est la vigilance d'un hacker honnête qui permet d'éviter le drame. Anthony Bouvet, de Montauban-de-Bretagne, est *pentester* freelance. Son job : éprouver la solidité informatique des entreprises. À titre bénévole, ce « cyber casque bleu » veille justement sur la sécurité des hôpitaux. Contrairement à ce qu'on espérerait, ils sont loin d'être des forteresses imprenables. « Les hôpitaux n'ont pas des moyens énormes pour blinder leurs fichiers sensibles. Il peut suffire de changer un chiffre dans l'adresse d'un site pour accéder à l'historique d'un patient. Une fois, ayant détecté une faille, j'ai fait un retour au prestataire du site qui avait décliné son application web à plusieurs établissements. » Laissant le champ libre à des attaques simultanées. Mais les plus grands ont aussi leur talon d'Achille, souligne Pierre-Alain Fouque, responsable du parcours Cybersécurité du Master Informatique de Rennes 1. « Avec une équipe, on s'est intéressé aux brèches de Whatsapp et d'autres produits grand public. Si les données sont mal protégées, il peut y avoir des fuites. Pas besoin d'un ordinateur extrêmement puissant pour mener ce type d'attaque. »

Avec la numérisation à tout crin des démarches administratives, ce sont désormais les collectivités locales qui sont visées par les pirates. Les villes n'ont pas toutes le réflexe ni les moyens de protéger la masse de données consenties par leurs administrés. Début 2016, quatre agents de Vannes ont introduit involontairement un virus dans le système de la Ville en ouvrant un e-mail piégé. Anthony Bouvet soupire : « En France, le niveau de cybersécurité n'est pas éminemment élevé. C'est pourquoi je veux l'améliorer à mon niveau. » ●



Des hackers n'hésitent pas à subtiliser les données de cliniques contre rançon.

COMMENT SE PROTÉGER

VPN
Ces réseaux privés virtuels renforcent l'anonymat sur Internet en masquant l'activité de l'utilisateur. Lisez bien les petites lignes et bannissez les services peu fiables qui stockent les données des clients.

Wifi publics
Un wifi gratuit auquel tout le monde peut se connecter, comme dans les gares, c'est pratique ! Mais rien ne garantit la sécurité de ces services.

Alias
Qui ne s'est jamais vu demander son e-mail au moment de créer une carte de fidélité ? Pour éviter la pub et d'éventuelles fuites, créez un « e-mail poubelle » que vous donnerez sans arrière-pensée.

Mot de passe
Les plus utilisés par les Français sont « 123456 », « bonjour » ou encore « motdepasse ». Des sésames crackables en une poignée de secondes. Préférez les phrases complexes d'au moins seize caractères -un logiciel de gestion des mots de passe aidera à les retenir.

Wikimedia - Kgbo