Les forbans des réseaux

Cécile Bontron, Le Nouvel Observateur Nº2276 - semaine du jeudi 19 Juin 2008

Hackers, crackers et pirates... Héros ambigus de la modernité, ils se jouent des sécurités informatiques pour défier le système. Mais aussi parfois pour s'enrichir frauduleusement. Quels sont les us et coutumes de ces étranges tribus ? Voyage au pays du hacking

Quatre mois de traque. Un filet qui s'est déployé en Ile-de-France, Midi-Pyrénées, Centre et Paca. Une bonne centaine de gendarmes mobilisés. Et le procureur de Dijon annonce, mercredi 28 mai, l'arrestation de vingt-deux personnes soupçonnées d'avoir piraté trente-quatre sociétés. Le premier réseau national de hackers jamais démantelé en France. *«Ils se retrouvaient sur un forum spécialisé et répondaient aux défis que leur lançait un webmaster*, raconte un enquêteur dijonnais. *Puis ils utilisaient des logiciels en libre circulation sur internet pour s'introduire au petit bonheur la chance dans les failles des systèmes informatiques des entreprises avant de se vanter de leurs exploits devant les petits copains du forum.»* Jusqu'à ce que la plainte d'une association de pêcheurs à la ligne bourguignons victime d'une de ces intrusions indélicates ne mette les enquêteurs sur la piste des ados...

Des hackers, vraiment ? Sur les forums et dans les chats, il est de bon ton de se moquer de cette petite bande désignée comme ennemi public numéro un. Des «lamers» *(débutants, NDLR)*, de vulgaires «script kiddies» même pas capables de mettre au point leurs propres logiciels, bref, des amateurs auxquels le noble nom de hacker ne saurait être accordé. Il n'empêche, les vingt-deux bidouilleurs qui échoueront sur le banc des prévenus dès le mois de septembre encourent des peines de prison avec sursis.
Dans le Far West du cyberespace, les frontières du bien et du mal sont encore mal définies. Apparu dans les années 1960 sur le prestigieux campus américain du MIT (Massachusetts Institute of Technologies), le terme de hacker désignait à l'origine les as de l'informatique capables de se jouer d'un programme, de le hacher selon l'étymologie anglophone, pour l'optimiser. Par la suite, avec l'explosion des réseaux, l'appellation a servi à désigner tous les bricoleurs passionnés animés de l'idéologie libertaire d'internet. Selon cette vulgate mondiale, l'information et les logiciels doivent être libres sur les réseaux. D'où l'idée, pour résister à toutes les puissances financières et administratives qui s'évertuent à contrôler le Net, de «craquer» les codes des logiciels, de s'introduire dans les bases de données et sur les sites. De faire voler en éclats les systèmes de sécurité qui cadenassent les programmes vendus sous licence. Ou de répandre des virus pour créer de jolies pannes informatiques. Tout est bon, en définitive, pour affirmer sa maîtrise technique et sa personnalité hors du commun, à la manière de Kevin Mitnick, sorte d'Arsène Lupin numérique devenu une icône mondiale. Ce teenager californien tombé dans la téléphonie et l'informatique s'est illustré en visitant les ordinateurs du Pentagone. Longtemps traqué par le FBI, il finira par écoper de cinq ans de prison pour le détournement des fichiers de Sun Microsystems, Motorola et Fujitsu, non sans avoir théorisé sa filouterie : «l'ingénierie sociale», qui permet aux hackers, en

abusant de la confiance de leurs interlocuteurs, de soustraire un mot de passe, un numéro de carte de crédit ou un accès aux systèmes informatiques... Aboutissement de cette mythologie, la figure du hacker s'est enrichie d'un personnage de fiction en passe de devenir très populaire : Lisbeth Salander, l'héroïne de la trilogie «Millenium», best-seller mondial du Suédois Stieg Larsson. Indomptable et surdouée du numérique, cette séduisante hackeuse utilise ses talents pour démasquer les industriels ripoux et les trafiquants de tout poil.

La réalité est un peu plus prosaïque. Car la philosophie du hacking ressemble plus au système D qu'à la «Déclaration universelle des droits de l'homme». *«Si tous les individus naissent libres et égaux devant le travail, ils ont aussi droit aux outils»*, résume Gob (1), qui a longtemps oeuvré dans un réseau de crackers *(voir notre lexique)*. Une véritable organisation clandestine. *«Le hacking est très élitiste, pas comme dans une entreprise. Si t'es mauvais, on ne te loupera pas»*, poursuit le jeune homme. Les sanctions sont immédiates : privation d'accès au serveur ou réduction des échanges. Gob avoue sans peine avoir été grisé par le sentiment de puissance que procure la maîtrise de la technique et du «système». *«Quand t'arrêtes, tu t'emmerdes.» «Le monde du hack - ou la «scène», comme ils disent - est une communauté d'experts qui se lancent des défis*, explique David Peyron, doctorant en sociologie. *Mais il faut beaucoup de temps pour être reconnu. On commence par des petits bouts de code qui ne servent à rien. Il y a aussi les coups d'éclat pour se faire un nom, mais sans frimer.» «Au début, je me suis fait remballer, on m'a dit :«Va voir sur Google»*, témoigne Adrien Retout, un ancien hacker. *Il faut faire ses preuves. Moi, j'avais des compétences en cryptologie. On est venu me chercher.»* Mais il faut dire qu'Adrien avait déjà réalisé quelques performances : hacker le compte MSN d'une fille pour tromper un ami, ou encore s'infiltrer dans le réseau d'une petite association de chefs d'entreprise. Avec ses propres outils. Respect...

Alors, bon ou truand, le hacker ? Certains se disent «white hats», ce sont les «blancs», les Robin des Bois qui ne s'introduisent dans les systèmes informatiques que pour mieux mettre en garde leurs utilisateurs des failles existantes. Pour Stéphane Koch, consultant et formateur en intelligence économique, *«ces hackers-là pointent les lacunes des systèmes de sécurité, dénichent les bogues dans les programmes. Ce sont eux, par exemple, qui ont montré que le passeport biométrique n'était pas assez sécurisé»*. D'autres, au contraire, se revendiquent «black hats», comme dans les westerns où les méchants portent des chapeaux noirs. Anars de l'ère numérique, ils attaquent les sites dans le but de casser, de provoquer des pannes et même de faire du chantage. «*Tandis que les «white hats» entrent chez vous pour jeter un coup d'oeil, les «noirs» vont s'amuser à repeindre les murs en rouge vif»*, compare Pierre-Loïc Doulcet, consultant en sécurité informatique.

En fait, le hacker et surtout ses agissements sont le plus souvent gris. Nicolas Sadirac est aujourd'hui directeur de l'Epitech, école d'informatique. Dans les années 1990, il a été l'un des hackers les plus emblématiques en France. Il a notamment accédé aux plans de l'avion Rafale, à la localisation de bases militaires, remplacé l'image de «la Joconde» sur le site du Louvre par une photo coquine... L'ex- hacker affirme : *«On ne se rend pas compte du mal que l'on peut faire. Même sans casser, on peut altérer une*

réputation, ou donner des idées à d'authentiques malfaiteurs. J'ai fini par réaliser que certains de mes camarades ont tiré profit de mes exploits.»
Avec l'explosion d'internet, la communauté du hacking a dû faire face à l'arrivée d'énormes enjeux financiers et politiques sur la Toile. *«Le crime organisé s'est converti au web, avec une professionnalisation accrue depuis deux ou trois ans»*, assure la criminologue Laurence Ifrah. Chantage, escroqueries, vols, les grands classiques de la pègre se retrouvent sur la Toile. Et même la guerre entre Etats : en avril 2007, l'Estonie a fait l'objet d'une attaque qui a paralysé pendant plusieurs jours des serveurs du gouvernement, mais aussi de banques, de médias et de partis politiques. On soupçonne une revanche russe.

Depuis deux ou trois ans, les experts en sécurité doivent aussi affronter l'espionnage économique. Les réseaux d'entreprises sont attaqués pour voler les plans ou les formules de futurs produits, pour épier les stratégies commerciales ou pour malmener les réputations. C'est principalement dans ce domaine que les hackers «black hats» sont recrutés, tels des mercenaires. Les spécialistes parlent alors de véritable piraterie. *«Il y a beaucoup d'argent à gagner*, affirme Christophe Casalegno, fondateur de Digital Network, société de sécurité informatique. *Pour une intrusion dans un laboratoire pharmaceutique, on peut toucher 500 000 euros à l'avance et 500 000 euros à la remise.» «Je fais ça pour le fric, pas pour le challenge technique»*, confirme Tripod (1). Ce pirate, qui tient à garder l'anonymat, est tombé du côté obscur de la force par opportunité : une proposition puis une autre. Tripod a tout fait : il a espionné des salariés pour leur propre patron, s'est introduit sur le réseau d'une institution européenne pour surveiller l'élaboration de nouvelles normes, saboté des réseaux... *«C'est la guerre économique»*, dit-il sans états d'âme.

Mais les «white hats» se professionnalisent aussi. Ils deviennent consultants en sécurité ! Adrien Retout a créé l'an dernier son entreprise d'intelligence économique, Proof of Concept. Ses activités ? *«Le «tracking», c'est-à-dire la recherche d'adresses d'un pirate, le «forensic», qui consiste à établir la preuve d'une intrusion, mais surtout des exercices de «black box», un test d'intrusion grandeur nature sans que personne, sauf le chef de la sécurité et le PDG, soit au courant.»* Ces simulations sont devenues l'apanage de spécialistes que l'on appelle les «ethical hackers» *(hackers éthiques, NDLR)*. On l'aura compris : dans cet univers impitoyable, l'amateurisme n'a plus vraiment sa place. Pourtant le sens du jeu n'a pas totalement disparu chez les ingénieurs en informatique. *«Mes étudiants tentent toujours de pirater le site de l'école»*, s'amuse Nicolas Sadirac, l'ancien flibustier devenu directeur. Petit hacker deviendra grand ...

(1)*Les pseudonymes ont été modifiés*.

Lexique

Hacker. A l'origine, programmeur de génie. Désormais, et surtout du fait des journalistes, désigne un pirate des réseaux.
Cracker. Il s'introduit dans un système ou un programme en détournant les mots de passe.
White hat. Il identifie une faiblesse dans la sécurité d'un système pour alerter les

gestionnaires.
Black hat. Ce pirate s'introduit dans un système informatique avec de mauvaises intentions.
Failles. Les systèmes d'exploitation comportent des faiblesses. «Statistiquement, sur un millier de lignes de codes, il y a vingt failles potentielles», indique Philippe Trouchaud, de la société de conseil PricewaterhouseCoopers.
Social engineering. Discipline qui consiste à berner son interlocuteur pour obtenir un mot de passe ou un code d'accès.

Cécile Bontron
Le Nouvel Observateur