« Le pirate informatique Rex Mundi, qui s'est attaqué il y a peu à l'opérateur Numericable, a en sa possession des données d'un demi-million de clients de Voo, a affirmé mercredi l'un des animateurs du blog Belsec, Len Lavens, devant la Commission de la Justice de la Chambre. » (http://www.rtbf.be/info/belgique/detail_hacking-voo-pirate-par-le-hacker-rex-mundi-selon-belsec?id=8108659)
Une demande de rançon aurait été envoyée à l'entreprise victime. Voilà ce que nous apprenait le site rtbf.be ce 9 octobre 2013. Déjà, en 2011, Nintendo était victime d'une tentative de chantage par un « hacker » ayant piraté ses systèmes et dérobé des données sensibles. Les pirates informatiques nous menacent ; les méchants « hackers » sont partout ; au secours !
Le terme « hacker » est donc synonyme de pirate informatique. Pour le grand public et la plupart des médias, oui assurément. Alors, je dis : halte là, mes gaillards, un peu d'étymologie et d'histoire s'imposent…
Ce mot semble être apparu pour la première fois vers 1959, au sein d'une association d'étudiants du MIT (Massachusetts Institute of Technology), le TMRC (Tech Model Railroad Club). À la même époque, les radio-amateurs utilisaient le terme « hacking » pour désigner une amélioration créative du fonctionnement d'un appareillage. Dans le monde de la recherche universitaire en informatique, le mot « hacker » a désigné les administrateurs réseaux, programmeurs, développeurs d'architectures matérielles d'ordinateurs ou encore les spécialistes en sécurité capables de faire preuve d'inventivité, voire de virtuosité. « Un hack désigne une combinaison ingénieuse, une invention à laquelle personne n'avait encore songé, que personne ne croyait possible avec les moyens du bord, un raccourci qui permet de faire plus vite et plus élégamment » (Mathieu Triclot in Philosophie des jeux vidéo, 2011). Toutefois, les premiers « hackers » se sont immédiatement trouvés en porte-à-faux par rapport au monde académique dans lequel ils évoluaient. Leur principe de base étant le libre accès à l'information, les règles strictes d'utilisation des matériels mis à leur disposition les indisposaient quelque peu… N'oublions pas qu'en ces années '50 et '60, les premiers ordinateurs installés dans les universités

avaient été conçus sous le contrôle et pour les militaires. Nous sommes aux débuts de l'ère informatique. Les machines électromécaniques de traitement de l'information datent de la Seconde guerre mondiale ou un peu avant. Mais c'est avec l'invention du transistor et son industrialisation dans les années '60 que le grand bond en avant de l'électronique va entrainer les chercheurs dans un développement technique en accélération constante. L'enthousiasme qui emporte ces jeunes techniciens et chercheurs les amène à repousser sans cesse les limites de leurs machines, à corriger les erreurs de conception… et à mettre les mains là où cela leur est interdit ! C'est ainsi que sont nés les premiers jeux vidéos (comme Spacewar en 1962), du détournement de machines destinées à des usages bien différents…
Une véritable communauté culturelle naît dans cette effervescence. Une communauté animée par une émulation permanente, une recherche constante du dépassement et une méfiance profondément enracinée à l'égard de toute forme d'autorité. Les « hackers » se créent alors une éthique qui sous-tend aujourd'hui encore leurs actions. Le journaliste américain, et spécialiste du domaine informatique, Steven Levy a codifié cette éthique comme suit :

- toute information est par nature libre ;
- il ne faut pas se fier à l'autorité, mais promouvoir la décentralisation ;
- les hackers peuvent se juger par leurs prouesses et non par d'autres hiérarchies sociales ;
- l'art et la beauté peuvent être créés à l'aide d'un ordinateur ;
- les ordinateurs peuvent changer la vie et l'améliorer.

L'apparition dans les années '80 des premiers ordinateurs personnels induira la démocratisation de l'informatique. Avec elle surviendra la naissance d'entreprises privées spécialisées dans le développement logiciel. De vastes communautés informatiques émergeront alors. Dans les années '90, le mouvement du logiciel libre verra le jour, sous l'impulsion de Richard Stallman, un ancien « hacker » du département de recherche en intelligence artificielle du MIT.

Historiquement, les « hackers » sont donc des informaticiens passionnés qui aiment pousser leur matériel dans ses derniers retranchements, cherchent des solutions innovantes et explorent de nouvelles voies. Tout cela en revendiquant une totale liberté d'action. A priori, il n'y a donc là rien de nuisible et dangereux ! Pourtant, les médias commettent souvent l'erreur de considérer que l'unique activité de ces individus est l'intrusion malveillante dans des réseaux et systèmes plus ou moins protégés. Dans le discours médiatique, le mot « hacker » est hélas devenu, systématiquement, synonyme de pirate informatique. Cette simplification outrancière aura sans doute été initiée par des journalistes pressés, à la recherche d'un terme générique facilement intelligible par le plus grand nombre. Il est vrai que le jargon informatique peut sembler obscur au profane… mais une trop grande simplification nuit à la compréhension. À moins que nous n'assistions, dans le chef de certains responsables médiatiques, à une forme de désinformation consistant à décrédibiliser une communauté libertaire et ses idées à contre-courant en la criminalisant aux yeux de l'opinion publique… (non, je ne suis pas adepte de la théorie du complot !) Plus simplement, ne sommes-nous pas témoins de l'étalage d'une certaine ignorance ?
Or donc, pour votre édification bonnes gens, permettez-moi de distinguer au sein de la grande famille des « hackers » :

- les « white hats » (chapeaux blancs) qui sont des professionnels de la sécurité informatique, qui réalisent des tests d'intrusion réseau légalement dans le cadre d'un contrat (ou illégalement afin d'avertir les responsables des failles de leurs systèmes) ;
- les « blue hats » (chapeaux bleus) qui sont des ingénieurs en sécurité testant contractuellement des logiciels et systèmes d'exploitation afin d'y détecter des failles et de les corriger ;
- les « grey hats » (chapeaux gris) qui pénètrent des systèmes illégalement sans volonté de nuire mais pour le plaisir de l'exploit ;
- les « black hats » (chapeaux noirs) qui sont des cyber-escrocs, espions, terroristes et créateurs de virus, et dont la motivation est principalement,

mais pas toujours, le profit ou le plaisir de nuire ;
- les « lamers » (faiblards) ou « script kiddies » (gamins du script) qui ne possèdent pas de grandes compétences et utilisent des techniques et programmes développés par d'autres pour pirater des systèmes (leur but est simplement d'attirer l'attention sur leur petite personne et acquérir une notoriété) ;
- les « hacktivistes » (hackers activistes) qui violent parfois la loi dans le but de défendre une cause.

Comme vous le constatez, la nébuleuse du « hacking » est étendue et ses contours un peu flous. Il peut sembler évident de qualifier de pirate un « hacker » qui dérobe des informations sensibles afin de les monnayer. Cela est plus discutable si l'individu dont on parle a percé les défenses d'un système par défi et n'a commis aucuns dégâts, n'a porté préjudice à personne. Le jugement est encore davantage sujet à caution si l'intrusion du « pirate » a mis en lumière une faille ignorée, induisant de la sorte une amélioration ultérieure de la sécurité. Gardons-nous de juger trop vite et, dans ce domaine comme dans d'autres, affranchissons- nous des termes réducteurs.

À bientôt, ici même ou AFK.