

Les nouveaux visages de la cyberdélinquance



L'analyse

Jacques-Olivier Martin
RÉDACTEUR EN CHEF DU « FIGARO » ÉCONOMIE

A en juger par les récentes et nombreuses attaques, l'insécurité gagne du terrain sur Internet. L'affaire Sony est dans tous les esprits. Depuis quelques semaines, la firme japonaise fait l'objet d'assauts à répétition, 16 au total, a affirmé hier un groupe de hackers. Le plus fameux a consisté à dérober les données d'abonnés à la plateforme de jeux PlayStation. Au total, Sony estime que 100 millions de comptes de clients ont été affectés. Il y a quinze jours, le groupe de défense américain Lockheed Martin annonçait de son côté avoir repoussé une attaque de grande ampleur menée par des hackers qui avaient préalablement dérobé des codes d'accès auprès d'un de ses fournisseurs. La semaine dernière, c'était au tour de Google de relater une attaque sur des comptes de sa messagerie Gmail.

Pour de nombreux spécialistes, cette cyberdélinquance devrait s'intensifier dans les années à venir. Plusieurs raisons à cela. « *Ce que nous voyons apparaître n'est que la conséquence de notre dépendance grandissante au numérique* », résume Nicolas Arpagian, auteur du « *Que sais-je ?* » *La Cybersécurité*. Chaque jour, en effet, de plus en plus de données sont mises en réseau, qu'il s'agisse des comptes bancaires, de données médicales, d'éléments fiscaux, de divers abonnements, de transmissions de données de la part d'entreprises. Une

cyberdépendance qui ne fait que susciter les convoitises.

Autre explication : l'accessibilité des armes. Il n'est plus nécessaire d'être un petit génie de l'informatique pour semer la terreur sur Internet. En se rendant sur des marchés aux voleurs virtuels, il est possible pour quelques centaines d'euros de louer les services de délinquants, de récupérer des codes confidentiels, de louer des réseaux d'ordinateurs, à l'heure, à la journée, au mois... pour mener des attaques. Il n'existe plus de barrières financières et techniques pour se lancer dans la cyberguerre.

Autant d'éléments qui rapprochent le monde virtuel de l'Internet du monde réel. La génération « *wargames* » des années 1990, qui menait des attaques sans cible précise, uniquement pour le panache ou pour porter à la connaissance de tous l'existence de failles, se fait plus rare. Le pirate a peu à peu cédé le pas au braqueur plus classique dont le principal objectif est l'enrichissement.

Les armes à sa disposition sont bien connues. Il s'agit notamment du hameçonnage, une technique qui consiste à se faire passer pour la banque d'un internaute afin d'obtenir ses identifiants et ses codes d'accès bancaires. D'autres recourent au Botnet, des réseaux d'ordinateurs zombies que l'on peut louer à l'usage pour récupérer des informations sur des cibles bien identi-

fiées et ensuite les revendre ou faire du chantage.

Au-delà de cette délinquance classique, Alain Esterle, chercheur associé à la Fondation pour la recherche stratégique (FRS), note depuis trois ou quatre ans la multiplication de tentatives de déstabilisation à grande échelle, qui s'apparentent à de la cyberguerre. En 2007, l'Estonie, pays alors très connecté, a subi une attaque massive qui a bloqué pendant plusieurs heures les services Internet des administrations, des banques, des médias. Le vrai défi pour les entreprises et pour les États est d'organiser la lutte contre une cybercriminalité terriblement difficile à vaincre. Les assaillants sont sans frontières, mobiles, peu identifiables.

Les sociétés multiplient les défenses informatiques et surtout échafaudent des scénarios pour arriver à se rétablir au plus vite en cas de déstabilisation. Quant aux États, ils se dotent depuis quelques années d'équipes opérationnelles capables de répondre, voire de mener des attaques. C'est le cas en France, au Royaume-Uni, en Allemagne. Les États-Unis ne ménagent pas non plus leurs efforts. Quelques heures après l'attaque contre Lockheed Martin, des responsables de l'armée américaine ont fait savoir que les cyberattaques seront désormais considérées comme des actes de guerre, ouvrant la voie à des ripostes militaires.

jomartin@lefigaro.fr



> 51

<<