Le Monde.fr

Les cyberattaques de l'été pourraient préparer des agressions plus massives
LE MONDE | 17.09.07 | 12h49 • Mis à jour le 17.09.07 | 15h02

Les attaques menées cet été par des pirates informatiques supposés chinois contre des *"services étatiques"* en France - mais aussi aux Etats-Unis, en Grande-Bretagne et en Allemagne - n'ont fait qu'augmenter les craintes sur une cybercriminalité en pleine expansion. *"J'ai du mal à croire que c'est une initiative de quelques petits génies à Hongkong. C'est extrêmement sophistiqué, cela a franchi toutes les protections"*, confiait à des journalistes le président de la République, Nicolas Sarkozy, dans l'avion qui le ramenait, vendredi 14 septembre, de Hongrie. Dans une note du 31 août, le Secrétariat général de la défense nationale (SGDN) aurait désigné la cible, deux adresses électroniques dépendant du ministère des affaires étrangères. Depuis, c'est l'inconnu.

La presse anglo-saxonne a relayé les soupçons portés contre des hackers (pirates) plus ou moins manipulés par l'armée populaire chinoise, et la France considère que les explications données par la Chine *"ne sont pas satisfaisantes"*. Mais aucune preuve ne peut être établie sur la provenance de ces attaques, toujours masquées, qui passent par un relais d'ordinateurs à travers le monde. Pour Laurence Ifrah, criminologue spécialisée dans la cybercriminalité, ces tentatives récentes sur une période de temps rapprochée ne sont pas de bon augure. *"Cela ressemble fort à des tests, pour mesurer la résistance des réseaux et les retombées médiatiques"*, affirme-t-elle.

Auteur de deux notes parues l'une dans la revue mensuelle de la défense nationale d'août-septembre, l'autre dans le numéro 70 de *Question d'Europe* de la fondation Robert Schuman du 3 septembre, cette chercheuse au Département de recherche des menaces criminelles contemporaines (DRMCC) de l'université Paris-II Panthéon-Assas, tire la sonnette d'alarme. *"Il faut désormais envisager*, écrit-elle, *la création de cellules nationales de surveillance, opérationnelle 24 heures sur 24, contrôlées par des professionnels aguerris aux techniques de contre-offensives."*

Cette veille existe déjà dans les services de la défense nationale, mais n'est pas assez développée à son goût depuis l'attaque massive déclenchée pour la première fois, contre un Etat, l'Estonie. Le 27 avril, après le déboulonnage d'une statue commémorant la victoire de l'armée soviétique sur les nazis, cet Etat balte a été la cible *d'"assauts uniques par leurs tailles et leur flux"* venus de Russie. *"Les effets dévastateurs sur les systèmes d'information visés* (des ministères et des banques surtout) *ont engendré une soudaine panique au plus haut niveau des Etats, de l'OTAN et de l'Union européenne"*, relève M^me^ Ifrah. Le système employé, Distributed Denial of service (DDOS) est redoutable. Il consiste, pour un ou plusieurs pirates, à envoyer un programme à quelques dizaines d'ordinateurs (appelés les "maîtres") qui sont à leur tour chargés d'infecter d'autres postes (les "agents"). Les machines ainsi "corrompues", sans que leurs utilisateurs n'en aient conscience, n'ont plus alors qu'à attendre les instructions du pirate qui déclenche l'attaque sans frontières. Le programme

employé pour l'Estonie se vendait à l'origine 700 dollars. Depuis, sa côte a grimpé à 1 000 dollars...

"PRISE DE CONSCIENCE"

Mais surtout, bien que très médiatisé, cet événement, souligne M^{me} Ifrah, *"n'est qu'un parmi près de 20 000 répertoriés entre septembre 2006 et janvier 2007"*. La criminologue évoque le cas de bookmakers britanniques rackettés par des pirates supposés russes, qui les auraient obligés à verser des rançons d'environ 50 000 dollars pour que cesse la saturation de leurs serveurs... *"Il y a manifestement une augmentation de ces faits"*, reconnaît Fabien Lang, commissaire de police, adjoint à la direction de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), rattaché à la police judiciaire, qui admet *"quelques affaires de racket de sociétés"* en France. Face à des attaques informatiques et *"tentatives de plus en plus fréquentes"*, Alain Juillet, haut responsable chargé de l'intelligence économique au SGDN, parle de *"prise de conscience"*.

Pour la seconde année, il se rendra aux Assises de la sécurité et des systèmes d'information prévues à Monaco du 10 au 14 octobre. Un marché en pleine expansion pour cet autre versant de la mondialisation.

Isabelle Mandraud
Article paru dans l'édition du 18.09.07