Pour McAfee, la guerre numérique est une réalité

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 18 novembre 2009

Spyworld Actu

Dans un rapport publié le 17 novembre, l'éditeur affirme que les attaques informatiques à but politique augmentent et que différents pays, dont la France, disposent de cyberarmes.

Les scénaristes de la série 24 h chrono travaillent-ils pour McAfee ? On peut se le demander à la lecture de la cinquième édition annuelle du Virtual Criminology Report rendue publique le 17 novembre 2009 par l'éditeur d'antivirus (télécharger ce rapport). Le constat établi dans ce document est alarmant puisque nous serions ni plus ni moins à l'aube d'une guerre numérique. « Au cours des vingt ou trente prochaines années, les cyberattaques feront de plus en plus partie de l'arsenal de guerre », déclare William Crowell, ancien directeur adjoint de la NSA, l'agence de la sécurité nationale américaine, dans le rapport.

Selon la vingtaine d'experts interrogés, majoritairement anglo-saxons, la course mondiale aux cyberarmes n'est plus une fiction. « Au cours des douze derniers mois, la progression des attaques informatiques à visée politique a déclenché l'alarme et suscité l'inquiétude, affirme McAfee. Rien qu'aux Etats-Unis, des attaques ont ainsi visé la Maison Blanche, le Département de la sécurité intérieure, l'U.S. Secret Service et le Department of Defense. »

Le grand public victime de la cyberguerre ?

Selon l'éditeur, des pays actifs dans la course au cyberarmement, comme la Corée du Nord et la Russie, mettraient au point des attaques contre des infrastructures majeures : réseaux de distribution de l'électricité, transports, télécommunications... « Quand on voit ce qui s'est passé en Géorgie, on sent bien que nous sommes à l'aube d'une guerre numérique. Ceux qui ont mené ces attaques étaient très bien renseignés », indique François Paget, chercheur en sécurité au sein de l'éditeur McAfee.

Mais le secteur privé est le plus exposé aux risques. « Il est dangereux pour les entreprises de croire que le gouvernement les sauvera en cas d'attaque majeure », explique Scott Borg, directeur de l'US-CCU (U.S.Cyber Consequences Unit), un institut de recherche indépendant.

Le grand public est aussi concerné part cette menace et de deux façons. « Premièrement, par rebond, il sera touché s'il y a de fortes perturbations dans le trafic aérien ou la distribution d'eau ou d'électricité. Deuxièmement, de nombreuses attaques mettent en oeuvre des botnets [réseaux d'ordinateurs contrôlés par des pirates, NDLR] et la plupart des PC impliqués sont ceux des particuliers », précise François Paget.

Mais ce rapport laisse dubitatif certains experts. C'est le cas de Daniel Ventre, ingénieur au CNRS et auteur du livre Information warfare (Ed. Wiley) : « Ce rapport n'apporte rien de nouveau. C'est une succession de lieux communs ou de points de vue très subjectifs, notamment sur l'affaire estonienne et le conflit russo-géorgien. Dans ce conflit par exemple, ce sont surtout des sites à valeur symbolique qui avaient été touchés. Les attaques concernaient essentiellement des défigurations de sites comme celui du ministère des Affaires étrangères et du parlement géorgien. Les atteintes aux systèmes d'information ont probablement eu un impact limité sur les capacités de la Géorgie en raison de sa faible dépendance aux systèmes d'information (7,5 % d'internautes en 2006). » Doit-on alors parler de cyberguerre, conclut le chercheur.

Post-scriptum :

http://www.01net.com/editorial/5086...