

Opération Titan RAIN : attaques massives depuis la Chine

Selon plusieurs sources officielles américaines relayées par le Washington Post, des sites web chinois sont utilisés de façon intensive pour attaquer des réseaux du département de la Défense US. Ces mêmes sources confirment que des centaines de réseaux non classifiés ont déjà subi des intrusions couronnées de succès. Pour ce qui est des réseaux sensibles, aucun d'eux n'aurait été compromis, mais les autorités restent vigilantes car des données anodines mises bout à bout pourraient bien donner quelques indices pertinents. Ces incidents, dont les premiers symptômes furent découverts il y a 2 à 3 ans, ont été baptisées « Titan Rain » par les agences de sécurité américaines. Toutefois, alors que quelques personnes au Pentagone sont convaincues de l'implication du gouvernement chinois dans ces tentatives d'attaques et d'espionnage de banques de données gouvernementales, d'autres y voient une simple volonté de cartographie de quelques 'hackers' déguisant leurs attaques derrière des réseaux chinois. «

*Ce n'est pas uniquement le département de la défense qui est touché mais bien une grande variété de réseaux incluant les réseaux des département d'Etat, de l'énergie et du Homeland Security» explique un officiel. Selon ce même témoignage, qui confirme que «C'est une tentative organisée et continue en vue de siphonner toute l'information contenue dans nos systèmes non classifiés ». Une autre source évoque cependant le fait que la portée de ces intrusions serait largement exagérée et que même si elles constituent effectivement un grand volume, ce n'est pas la chose la plus préoccupante. Si l'existence de « Titan Rain » a bien été admise ainsi que les quelques informations publiées, les officiels qui ont été interviewé ont refusé d'en dire plus pour des raisons légales et politiques mais également pour éviter de donner trop d'informations aux hackers. Enfin, l'ouverture d'une enquête officielle par le FBI a fait l'objet d'un « no comment » très évasif ? Au mois de juin dernier une section séparée d'un rapport du secrétaire à la défense US Donald Rumsfeld était déjà entièrement consacrée au développement des systèmes d'attaques informatiques des militaires chinois. Il y est évoqué que l'Armée de Libération du Peuple considère que les opérations sur des réseaux d'ordinateurs sont « critiques pour prendre l'initiative » dans l'établissement d'une « domination électromagnétique » dans les premiers instants d'un conflit en vue d'une meilleure efficacité lors de la bataille. Des unités spécialisées auraient de plus été créées dans les secteurs de la guerre de l'information et la création de virus avec pour objectif d'attaquer les systèmes et réseaux ennemis mais aussi des tactiques de protection des systèmes alliés. Suite à cet assaut, un nouvel élan aurait été donné du côté du Pentagone pour mettre en place de nouveaux programmes de détection d'intrusion et de formation d'experts en sécurité. **Cédric Messeguer pour Vulnerabilite.com***

Arrestations au Brésil

L'Opération Pegase est un succès. Menée au Brésil par 410 policiers fédéraux dans sept Etats du pays, elle a permis l'arrestation de 80 pirates spécialisés dans le 'phishing' et autres arnaques bancaires. Ces personnes sont accusées d'avoir volé plus de 33 millions de dollars en piratant les comptes bancaires en ligne d'internautes insouciantes, ont annoncé les autorités. Pourtant, la plupart des Brésiliens n'ont pas d'ordinateur à domicile, mais des études montrent que ceux qui en possèdent sont parmi les internautes les plus assidus au monde, surtout en matière de gestion de

leurs comptes en banque. Et ça, les pirates l'ont bien compris. Le mois dernier une étude menée par le comité brésilien Computer Emergency Response Team montrait que les plaintes pour fraudes en ligne dans le pays avaient bondi de 1.300% au deuxième trimestre, grimant à 7.942 cas contre 562 l'année précédente.