Sécurité : la Chine souhaite plus de collaboration

Une étude, réalisée par des militaires chinois affirme que le pays est devenu une cible privilégiée des hackers. En publiant ce document, le gouvernement essaye de s'exonérer des soupçons qui pèsent sur lui quant aux récentes attaques lancées contre plusieurs pays, dont l'Allemagne, la France et les États-Unis. Interrogé par l'agence officielle Xinhua news agency, l'auteur de ce document, Wang Xinjun, a expliqué :*« les pays qui sont victimes de ces attaques devraient collaborer au lieu d'accuser. » « Les attaques menées en Chine ont explosé ces dernières années, et selon moi notre pays est bien plus exposé que la plupart des pays occidentaux. Pourtant, notre gouvernement n'accuse jamais ces pays d'être à l'origine de ces attaques, il préfère insister sur l'urgence d'une plus grande collaboration internationale contre la cybercriminalité. »* Xinjun s'étonne des accusations faites par les gouvernements européens selon lesquelles la Chine essaye d'attaquer ces systèmes. Pour lui rien ne prouve qu'elles ont été commanditées par le gouvernement, une affirmation confirmée par plusieurs experts de la sécurité informatique. Pour Wang, il est essentiel de mettre un terme à cette relation digne de « la guerre froide ». *« Les pays doivent se donner plus d'informations sur les hackers et collaborer davantage pour mettre une terme a ce phénomène. »*

La France dans le giron des hackers chinois? Interrogé sur la récente attaque chinoise qui a touché la France, Laurent Heslault, responsable de la zone EMEA chez Symantec donne son point de vue : ***-Le terme de « cyber-guerre mondiale » est-il approprié? Combien de pays sont en guerre, quels sont les exemples les plus frappants?*** Je ne pense pas que l'on puisse parler de « cyber-guerre mondiale » à l'heure actuelle. Même si certains exemples, comme les cyber-attaques dont l'Estonie a été victime en avril dernier, montrent la forte dépendance des sociétés modernes envers les systèmes d'information. Certains pays, comme les Etats-Unis se sont dotés ouvertement de corps d'armée spécialisé dans la défense et même l'attaque des infrastructures informatiques. ***-Quel serait l'impact d'une attaque réussie contre l'infrastructure informatique française, sur l'économie et sur la sécurité du pays ?*** Difficile à dire, dans la mesure ou les niveaux de protection sont différents d'une entreprise ou organisation à l'autre. On peut noter cependant que d'après un rapport Symantec sur la gestion du risque, ce sont dans les environnements potentiellement les plus exposés que l'on trouve les organisations les plus conscientes des risques et par conséquent souvent les mieux préparées.

–Dans le cas de la récente attaque qui a touché la France, peut-on affirmer que les hackers travaillaient pour le gouvernement chinois ? Quels sont les éléments qui permettent de statuer ? Les éléments communiqués publiquement par le SGDN (Défense nationale), même s'ils indiquent que l'attaque venait de Chine, ne permettent en aucun cas d'aller plus loin. En effet, la machine « source » pouvant facilement être contrôlée à distance. Je rappelle que, d'après le dernier rapport semestriel de Symantec sur l'évolution des cyber-menaces, près de 30% des » pc-zombies » détectés dans le monde l'étaient en Chine, alors que 43% des serveurs contrôlant ces mêmes « Bots » (les « Command&Control Servers ») étaient localisés aux Etats-Unis ; eux-mêmes potentiellement pilotés depuis une autre machine n'importe où sur la planète? ***-Les terroristes ne risquent-ils pas de s'inspirer de ces attaques ou bien faut-il nécessairement l'appui d'un gouvernement pour mener des attaques d'une telle ampleur ?*** D'une manière générale, la

propagation des techniques est une des caractéristiques de la cyber-criminalité. Cependant, il est très difficile d'imaginer aujourd'hui qu'un pays puisse être derrière les campagnes de spam ou de phishing qui nous impactent quotidiennement, bien que l'ampleur en soit conséquente. Certains réseaux de « pc-zombies » ou « BotNets » sont à louer et à disposition de qui voudra payer.

-Estimez-vous que désormais ces attaques vont se multiplier ? D'une manière générale, la multiplication d'attaques va de paire avec le succès rencontré. Certains types d'attaques sont abandonnés au profit d'autres, plus efficaces. Le taux de détection des attaques rentre également en ligne compte. En effet, difficile d'apprécier l'évolution d'attaques que l'on ne détecte pas? ***-Quid des principales cibles des hackers? Quelles sont-elles? Sait-on ce que les hackers chinois cherchent ? Peut-on identifier les cibles stratégiques ?*** *La principale motivation est clairement financière. Tout ce qui pourra aboutir, à court, moyen ou long terme, à un profit quelconque est envisagé. Le vol d'identité pour usurpation est en tête de liste. On en veut à nos informations. Rien ne nous permet cependant d'affirmer que tel ou tel pays pourrait encourager à attaquer un type de cible plutôt qu'un autre.*

-Le niveau de sophistication des attaques prouve-t-il l'implication du gouvernement chinois ?

Nous n'avons aucune information permettant de répondre à cette question. ***-Si on ne peut pas retrouver les responsables comment empêcher que ces attaques se reproduisent ?*** *En terme de prévention, il est fondamental de passer de la tactique à la stratégie, et de favoriser une sécurité pro-active, tournée vers la gestion des risques. L'éducation et la sensibilisation des personnes est également incontournable.* ***-La réponse de la Chine selon laquelle elle aurait été victime d'attaques est-elle recevable ?*** *Impossible à savoir pour le moment* ***-Existe-t-il un profil type du hacker ? À votre avis, il s'agit d'amateur, de professionnel, ou bien la méthodologie utilisée est elle militaire ?*** *Il est clair que ces dernières années le profil a évolué de l'amateur au professionnel. Symantec a observé une professionnalisation, voir une commercialisation accrue de ces activités malveillantes. L'émergence d'un écosystème basé sur les échanges, via une économie clandestine, a favorisé la collaboration et la segmentation en différents « métiers » : « Recherche de vulnérabilités », « développement de code malveillants », « recherche d'adresses de messagerie », « Spammeurs », « mules »?*