Note de Veille Cyber n°1

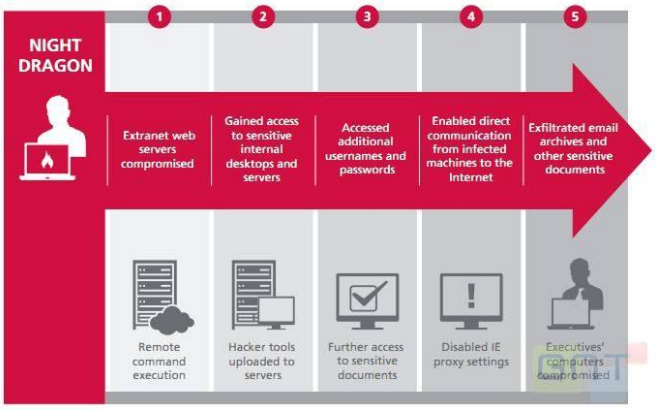
Du 1 au 11 février 2011 par Alix Desforges

Note préalable à la lecture : du fait de la nature du sujet et de l'intérêt d'une note conçue à l'appui de l'ensemble des sources d'information disponibles sur le web (blog, journaux, etc.), la totale fiabilité des informations proposées ne peut être pleinement garantie. Cette note propose d'ouvrir des perspectives. A chacun de poursuivre le travail.

Piratage

Night Dragon ou l'espionnage des sociétés d'énergie. Source

La société McAfee a mis à jour une campagne d'espionnage « coordonnée, discrète et ciblée » visant des multinationales du secteur de l'énergie et du pétrole. L'éditeur de solution de sécurité a pu remonter la piste jusqu'en Chine, se gardant bien, toutefois d'évoquer l'implication du régime chinois. La compromission de serveurs de contrôle-commande aurait ainsi permit le vol d'informations confidentielles depuis 2007.



Source : www.generation-nt.com

Le NASDAQ piraté depuis plus d'un an. Source

La société NASDAQ a révélé que son système a été pénétré à plusieurs reprises pendant un an. Si ces intrusions n'ont pas affecté la plateforme de cotation directement, elles ont visé une application en mode SaaS appelée Directors Desk qui contient des données confidentielles sur les sociétés présentes sur le marché américain.

Organisation et doctrine des armées

L'Australie bientôt en partenariat avec l'OTAN sur la cyberdéfense. Source

Le Ministre de la Défense australien, Stephen Smith, a rappelé l'engagement de son gouvernement dans la mise en place d'un accord avec l'OTAN sur la cybersécurité et la cyberdéfense. Le partenariat doit se faire dans le cadre du Concept Stratégique pour la Défense et la Sécurité des membres de l'OTAN.

L'US Navy se prépare à mener des opérations dans le cyberespace. Source

L'US Navy Space et le Naval Warfare Systems viennent de signer un contrat avec quatre entreprises dont Northrop Grumman Systems Corp. et Booz Allen Hamilton Inc. Evalué à 311 millions de dollars pour la première année (phase d'évaluation des architecteurs existantes et des besoins en opération), le projet pourrait avoisiner le milliard de dollars au cours des trois prochaines années pour l'implémentation des systèmes conçus.

Le recrutement de pirates en vogue dans les armées. Source Source

Cyber Fast Track est un projet de la DARPA visant à utiliser et intégrer les capacités de la communauté des pirates informatiques dans les projets de l'agence. L'armée israélienne aussi a manifesté l'intention de s'attribuer les services de 120 hackers. D'après le porte parole de l'armée, le Premier Ministre Benjamin Netanyahu aurait personnellement apporté son soutien au projet et lui aurait attribué un budget de 1.63 millions de dollars.

Menaces

La Conférence de Munich sur la sécurité met l'accent sur les cybermenaces. Source

La conférence (du 4 au 6 février 2011) qui a notamment rassemblé le Premier Ministre britannique David Cameron, la Chancelière allemande Angela Merkel, la Secrétaire d'Etat aux Affaires Etrangères américaine Hillary Clinton ou encore le Ministre russe des affaires étrangères Sergei Lavrov, a mis l'accent sur le besoin d'établir des règles d'engagement dans le

cyberespace. L'ensemble des dirigeants se sont accordés sur le besoin d'établir une politique internationale pour lutter contre les cyberattaques. Le think tank EastWest Institute a publié à cette occasion une étude évoquant l'instauration d'une convention pour le cyberespace du type de celles de Genève ou de la Hague. Rappelant l'importance de l'implication du secteur privé dans cette démarche, le rapport évoque les difficultés d'attribution des attaques et en particulier de déterminer l'implication d'un Etat dans celles-ci.

Un rapport commandé par le Président Obama pointe les lacunes des Etats-Unis en matière de cybersécurité. Source

Le Center for Strategic and International Studies dresse un bilan bien pâle des efforts réalisés par les Etats-Unis en matière de cybersécurité. Le rapport regrette que la situation économique ne favorise pas l'émergence de politiques volontaristes dans le domaine alors que plusieurs évènements majeurs ont rappelé le manque de cybersécurité (Opération Aurora, Stuxnet, Wikileaks…). Le CSIS émet dix recommandations pour pallier ces menaces d'ici les deux prochaines années.

Initiatives

Le Canada établit un plan de route pour sa stratégie de cybersécurité. Source

Le plan détaillé par le Ministre de la Sûreté publique canadien doit permettre la coordination aux différents niveaux de gouvernement et avec l'implication du secteur privé d'une politique cohérente pour faire face aux cybermenaces. 90 millions de dollars seront ainsi investis sur cinq ans par l'Etat fédéral et financeront les politiques mises en œuvre qu'il s'agisse de prévention ou de l'élaboration d'un Plan de Continuité d'Activité.

La Turquie organise une simulation de cyberattaque. Source

La Turquie a organisé du 25 au 28 janvier un exercice d'attaque informatique auquel participaient plus de 30 institutions de l'Etat. Conduit par l'Autorité des technologies de l'information et de la communication (le BTK), le Conseil national de recherches scientifiques et techniques (le TÜBITAK), le Centre de recherche pour les technologies avancées en informatique et sécurité de l'information (BILGEM) et l'Institut National de Recherche électroniques et cryptologie (l'UEKAE), l'exercice visait à préparer la Turquie à faire face à des cyberattaques. Il s'agissait principalement d'évaluer les capacités de réponse des institutions.

Publications récentes

- *EastWest Institute,* Working towards rules for governing cyber conflict, rendering the Geneva and Hague Conventions in cyberspace*, février 2011*
- *CSIS,* Cybersecurity two years later*, Report of the CSIS commission on cybersecurity for the 44th presidency, janvier 2011*
- *Peter Sommer et Ian Brown,* Reducing Systemic Cybersecurity Risk*, OCDE, janvier 2011*
- *Martin Libicki,* Chinese use of cyberwar as an anti-access strategy*, RAND Corp, janvier 2011*

Evènements

Conférence RSA du 14 au 18 février à San Francisco