Cyber-espionnage : un nouveau rapport pointe les liens entre les hackers et l'armée chinoise

En pleine guéguerre de communiqués entre la Chine et les Etats-Unis, un **rapport de la société californienne CrowdStrike** vient apporter de l'eau au moulin des autorités nord-américaines. Selon cette étude, un groupe de hackers chinois, Putter Panda, aurait des liens directs avec l'armée chinoise. CrowdStrike base ses conclusions sur un certain nombre de posts sur Internet, upload de photos et surtout enregistrements de noms de domaine réalisés par un membre de ce groupe de pirates : **Chen Ping, alias cpyy**. Selon la société de sécurité, ce dernier travaille en fait dans les bureaux d'une unité spécialisée dans le cyber-espionnage de l'armée chinoise, **l'unité 61486 basée à Shangai**. Il n'en aurait pas moins enregistré les noms de domaine des serveurs de contrôle et de commande d'un malware mis en œuvre par Putter Panda.

Actif depuis au moins 2007, ce groupe de hackers s'est notamment attaqué aux **sociétés nord-américaines et européennes spécialisées dans l'aéronautique et les satellites**. Les techniques mises en œuvre reposent sur des exploits pour des applications de productivité standards, comme Microsoft Office ou Acrobat Reader, des malwares déployés via des campagnes d'e-mails ciblés.

Un flot d'accusations mutuelles

Selon Crowstrike, « *il est probable que cette organisation (Putter Panda, NDLR) soit formée en partie par des étudiants ou anciens étudiants de la STJU (une université chinoise utilisée par l'armée chinoise pour recruter des spécialistes de cyber-intelligence, NDLR) et partage des ressources et des directives avec l'unité 61398 de l'armée populaire de Chine* ». Cette seconde unité avait été pointée du doigt dès février 2013 dans un rapport d'une autre société américaine, Mandiant, là encore pour ses liens présumés avec un groupe de hackers pratiquant le vol de données commerciales.

Rappelons que, vers la mi-mai, **la justice américaine a officiellement inculpé cinq militaires chinois** pour « *piratage informatique* » et « *espionnage industriel* » à l'encontre de six entreprises américaines. Dans une interview récente à un journal australien, le **général Keith Alexander**, ex-directeur de la NSA américaine, expliquait : *« L'espionnage contre nos sociétés privées, contre nos ressources de R&D ou contre toute autre cible intéressante pour un compétiteur international a atteint une échelle industrielle. Son étendue est bien supérieure à ce que les gens imaginent. En fait, je pense que la propriété intellectuelle qui a été dérobée aux Etats-Unis depuis une décennie ou deux représente le plus grand et le plus rapide transfert de richesses involontaire de l'histoire de l'Humanité. »* Et de nier, dans la foulée, toute pratique d'espionnage économique par la NSA sous sa direction (entre 2005 et mars 2014).

Un audit de sécurité pour les produits US

La Chine avait alors qualifié d'hypocrites ces accusations, pointant les pratiques de la NSA mises au jour par Edward Snowden. Et avait annoncé la mise en place prochaine d'un nouveau « *système*

d'enquête de cybersécurité » auquel devront se soumettre les produits avant d'être vendus sur le territoire de la seconde économie mondiale. Objectif affiché : détecter les systèmes qui **permettraient l'espionnage des intérêts chinois** par des puissances étrangères. Une mesure qui cible clairement les intérêts économiques américains.

Un rapport de l'**Académie chinoise du cyberespace avait ensuite accusé Washington** de cyber-espionnage *« sans scrupule »* via des attaques informatiques de *« grande ampleur ». « La surveillance américaine a pour cible le gouvernement et les dirigeants chinois, les sociétés chinoises, les instituts de recherche scientifique, les citoyens ordinaires et un grand nombre d'utilisateurs du téléphone mobile »,* écrivait ce rapport.

Lire également :

La NSA pratique aussi l'espionnage économique, d'après Snowden
NSA : les matériels Cisco, Juniper et Huawei transformés en passoire