Des experts en sécurité détaillent un piratage de grande ampleur aux États-Unis

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 25 novembre 2005

Un groupe de pirates, présumés Chinois, ont perpétré une série d'attaques visant des sites d'information américains sensibles. Différentes centres de l'armée et la NASA ont été en ligne de mire de ce vaste piratage, qui s'est étalé entre 2003 et 2004.

Un expert en sécurité du SANS Institute a dévoilé de nouvelles informations sur des vols répétés de documents sensibles, dont ont été notamment victimes, en 2004, des bases de l'armée américaine, ou encore la Nasa.

Le commando informatique, baptisé "Titan Rain" par le gouvernement américain, serait composé de vingt Chinois basés dans la province de Guangdong. Ils ont réussi à pénétrer des réseaux informatiques et à s'emparer, entre autres, de spécifications techniques.

« Ils ont obtenu, depuis l'arsenal Redstone, base de l'aviation militaire et du centre de commandes de missiles, les spécifications d'un système de plans de vol pour les hélicoptères de l'armée, ainsi que le logiciel de planification des vols Falconview 3.2 utilisé par l'armée et l'US Air Force », a indiqué Alan Paller, le directeur du SANS Institute lors d'une réunion au ministère du Commerce et de l'Industrie britannique, à Londres.

Ces vols auraient débuté en 2003. Une attaque massive a eu lieue en novembre 2004, rendue publique seulement cet été. Le quotidien américain Washington Post a rapporté que des sites web chinois étaient utilisés pour cibler des réseaux informatiques du ministère de la Défense et d'autres agences américaines.

Selon Alan Paller, pendant la nuit du 1er novembre 2004, les pirates ont d'abord exploité des failles dans le poste de commandes du système d'information de l'armée américaine, à Fort Huachuca (Arizona). Ils ont ensuite tiré parti de la même faille dans les ordinateurs de la DISA ; cet organisme administre des portions du réseau internet qui entrent dans la composition du réseau militaire, à Arlington, Virginie. Puis ils s'en sont pris à une installation de la marine américaine à San Diego (Californie). Avant de pénétrer un autre site traitant des questions spatiales et stratégiques à Huntsville (Alabama).

Des portes laissées ouvertes pour pouvoir revenir

Le magazine Time a lui aussi relaté l'affaire, indiquant qu'un expert en sécurité américain du ministère de l'Énergie, Shawn Carpenter, avait repéré le manège des Chinois. Les pirates ont laissé des portes d'accès pour pouvoir revenir. Il a réussi à remonter jusqu'à eux, en pénétrant des routeurs en Chine. Il a pu enregistrer des sites ayant été corrompus, et découvert des données volées par les pirates. Il a ensuite transmis ses informations à l'armée et au FBI, mais s'est fait licencier par son employeur pour piratage informatique.

Le directeur du SANS Institute estime que le bénéficiaire des données récoltées n'est autre que le gouvernement chinois. « Bien sûr que c'est le gouvernement. Les gouvernements donneraient tout pour prendre le contrôle des ordinateurs d'autres gouvernements. C'est bien plus efficace que d'effectuer des écoutes téléphoniques. »