

Extrait du Spyworld Actu

<http://ks3094133.kimsufi.com/spip.php?article2920>

# USA : Premières cyber attaques contre des centrales

- Terrorisme - International -



Date de mise en ligne : lundi 6 novembre 2006

---

Spyworld Actu

---

**Le FBI est en pleine phase d'investigation suite à l'attaque par un pirate étranger d'une centrale de traitement des eaux à Harrisburg, Pennsylvanie. Cette centrale a été l'objet d'un piratage matérialisé par l'implantation d'un logiciel malicieux qui aurait pu affecter gravement les opérations de traitement de l'eau.**

Les officiels sont formels, le pirate n'a pas tenté de prendre le contrôle global du système, mais bien de l'utiliser à son propre bénéfice pour y déposer et distribuer des emails et des logiciels piratés.

Cependant, l'agent spécial Jerri Williams du bureau local du FBI à Philadelphie souligne que « le risque était majeur car le PC concerné contrôle une infrastructure système sensible qui aurait donc pu entraîner une interruption de service ».

Le pirate a commencé par s'introduire sur l'ordinateur portable d'un employé, puis a utilisé son accès à distance comme point d'entrée. Une fois cette intrusion réalisée, il a mis en place un virus et un spyware sur le réseau de l'usine de traitement des eaux. « Ce genre d'attaque est très commun en fait, tous les pirates essaient de prendre le contrôle de différents systèmes pour les utiliser notamment comme relais de spam. Et rien n'indique que ce piratage ait été réalisé pour une autre raison », raconte l'agent Williams.

Tous les mots de passe ont bien évidemment été changés après l'attaque et les accès à des fins de télétravail désactivés.

### **Les attaques se multiplient**

Lors d'une des attaques précédentes, les pirates avaient utilisé un opérateur telecom coréen pour lancer une attaque de dénis de service sur une centrale hydraulique. Un second cas fait lui aussi état d'une intrusion au coeur du système de contrôle et d'acquisition des données d'une centrale d'épuration en Californie et enfin, dans un troisième cas, les protagonistes ont laissé leur message évocateur « Je suis entré dans votre serveur comme vous l'avez fait en Irak ».

Diane Van De Hei, la directrice du WaterISAC est formelle, « Nous constatons une augmentation croissante des rapports sur ces cas de piratages », alors qu'avant le 11 septembre 2001, la majorité des entreprises géraient ces attaques en interne sans en faire état.

Le WaterISAC (Water Information Sharing and Analysis Center) est un système d'alerte couplé à un portail sécurisé né de la volonté, post 11 septembre, de se prémunir non seulement contre les attaques terroristes mais aussi contre les cyber-terroristes.

Ce système, mis en place depuis Décembre 2002, est principalement orienté vers ses membres qui comptent parmi les 1000 stations de traitement des eaux et d'épuration des Etats-Unis. Il est cofinancé par le biais d'un abonnement annuel proportionnel au nombre et à la taille des populations à protéger, ainsi que par des fonds du Congrès américain et de l'agence de protection de l'environnement (EPA).

Les abonnés de ce système peuvent ainsi bénéficier d'une sécurité orientée métier améliorée, de coûts d'assurance

## USA : Premières cyber attaques contre des centrales

---

réduits, d'un système d'alerte 24/7 et enfin de l'accès à des experts dans les domaines de la sécurité à mettre en place dans le domaine de l'eau.

*Post-scriptum :*

<http://www.vulnerabilite.com/actu/2...>