Attaque informatique russe contre le secteur de l'énergie

01/07/2014 à 22h57

Un groupe de pirates informatiques russe qui se fait appeler « *Energic Bear* » attaque depuis maintenant plusieurs semaines des centrales nucléaires occidentales avec un malware qui pourrait perturber l'alimentation en électricité. Selon plusieurs chercheurs en sécurité informatique l'objectif principal serait l'espionnage industriel, mais le logiciel permettrait également aux pirates de prendre le contrôle des systèmes à distance.

Il serait ainsi éventuellement en mesure de saboter les installations, ou pire de couper l'alimentation électrique, des citoyens et d'entreprises de certains pays occidentaux.

> ***Les premières attaques auraient été découvertes en 2012, selon les chercheurs de CrowdStrike, et auraient déjà affecté 2000 organisations dans 84 pays.***

La société basée en Californie a depuis observé d'autres attaques similaires particulièrement sophistiquées contre des organismes de santé, des sociétés travaillant dans la défense, ainsi que des organismes gouvernementaux.

Les enfants de Stuxnet

Aujourd'hui, c'est l'entreprise de sécurité informatique Symantec, qui a baptisé ce malware Dragonfly, qui affirme que ce groupe de pirates peut désormais prendre le contrôle de puissantes structures.

Symantec déclare ainsi que parmi les cibles de ce groupe, on retrouve des gestionnaires de réseaux d'énergie, de grandes entreprises électriques, des exploitants de pipeline de pétrole et de gaz, ainsi que des fournisseurs en équipements industriels de l'industrie énergétique.

La majorité des victimes étaient situées aux États-Unis, en Espagne, en France, en Italie, en Allemagne, en Turquie et en Pologne. Bien évidemment, les hackers n'ont pas laissé de traces grâce à l'utilisation de techniques de cryptage avancées.

La société F-Secure indique quant à elle que le groupe de pirates est devenu depuis environ six mois plus agressifs et que leur manière d'agir s'est sophistiquée.

Cette vague de piratage est similaire à celle mise en place en 2010 par les États-Unis et Israël avec le virus Stuxnet créé dans le but d'endommager l'industrie nucléaire iranienne.

Daily Geeks