# Piratage des SCADA, cessez de prendre des selfies !

Les récentes attaques contre les opérateurs d'électricité Ukrainien ou l'aéroport de Kiev montrent clairement que les infrastructures essentielles ou critiques sont la cible de cyber-saboteurs. Des spécialistes qui prennent le temps de comprendre, d'analyser et de planifier leurs attaques. Les gouvernements se livrent donc à une course contre la montre pour recenser et sécuriser l'informatique industrielle et notamment les systèmes SCADA.

En France, l'ANSSI mène depuis plusieurs années des travaux avec les industriels et les fabricants de systèmes informatiques dédiés. Le fruit de ces travaux est intégré dans la Loi de Programmation Militaire (LPM) avec la création des opérateurs d'importance vitale (OIV) qui vont être obligés de sécuriser les parties de leur SI les plus critiques. On attend toujours la publication des arrêtés sectoriels pour connaître les contraintes techniques et le périmètre des équipements visés.

Pour autant, il n'est pas sûr que, dans les obligations de l'ANSSI, on trouve la recommandation de Sean Mc Bride, analyste senior en Threat Intelligence chez iSight . **« *Pas de selfies de SCADA* »**, a scandé le consultant lors de la conférence S4 qui s'est tenue à Miami, avant d'ajouter : « *Ne rendez pas plus facile le travail des adversaires.* » Une alerte lancée après que la firme de sécurité ait trouvé sur différents réseaux sociaux (Facebook et Instagram) des photos des lieux de travail (centrales électriques, traitement des eaux, etc.) ou des portraits de personnes devant des systèmes SCADA par exemple.

## Une mine d'informations à portée de vue

Des prises de vues anodines mais qui peuvent donner des éléments précieux pour des pirates. Ainsi, iSight a découvert des **photos panoramiques d'une salle de contrôle** et même une **vidéo d'une promenade à travers des installations**. Un attaquant peut ainsi trouver plusieurs informations, le nombre et le type d'équipement, les connexions entre eux, des plans, des listes du personnel affichées sur un tableau (un moyen de cibler une personne en particulier pour entrer dans le système), explique Sean Mc Bride. Au total, le consultant et une équipe de chercheurs ont réussi à glaner des informations issues de différentes sources (médias sociaux, entreprise et administration) et référencer 15 centrales électriques aux Etats-Unis.

L'utilisation des photos a déjà été éprouvée dans le cadre de la première attaque connue de système industriel : Stuxnet. En 2008, le service de presse de l'ancien président iranien Mahmoud Ahmadinejad publie une photo le montrant devant des ordinateurs et se promenant à l'intérieur de la centrale des centrifugeuses de Natanz. A l'époque, l'Iran est fortement soupçonné de vouloir enrichir de l'uranium à des fins militaires. Des Etats (probablement Etats-Unis et Israel) ont décidé de lancer une attaque pour saboter cette centrale en visant les systèmes industriels SCADA. Les photos prises par le service de presse avaient, selon un chercheur, permis de déterminer, sur la base des images des écrans d'ordinateurs, le nombre de centrifugeuses présentes dans le bâtiment.

**A lire aussi :**

Scada : une cyberattaque peut-elle faire dérailler un train ?
Les 10 principales défaillances des systèmes Scada selon Lexsi

**Crédit Photo : Genkur-Shutterstock**