Cyberattaques contre l'écosystème des centrales nucléaire américaines

Selon le *New York Times*, le ministère de l'intérieur et le FBI ont lancé une alerte « ambre » aux industries nucléaires américaines. Ce niveau d'alerte est le second niveau le plus élevé pour ce type de rapport.

Il fait suite à une vague de cyberattaques visant des prestataires gérant des centrales nucléaires. Parmi eux, le rapport cite Wolf Creek Nuclear Operating Corporation, qui gère notamment la centrale nucléaire du Kansas. Les offensives ont débuté en mai, mais les autorités américaines n'ont averti les industriels que très récemment.

Le rapport précise que les PC des employés étaient visés à travers une campagne intense de phishing. Les ingénieurs en charge du contrôle des installations nucléaires étaient visés, via l'envoi de faux CV provenant de gens ayant les mêmes profils. Le FBI et le DHS (*Department of Homeland Security*) rappellent que les réseaux des employés et industriel sont bien isolés les uns des autres. De plus, les réseaux de contrôle sont accessibles en mode « air gap », c'est-à-dire non connecté à Internet.

Energetic Bear derrière les attaques ?

Cela ne signifie pas pour autant, qu'ils sont complétement sécurisés. Une étude anglaise de 2015, citée par nos confrères d'*Ars Technica*, montre que ces systèmes de contrôle ne sont pas « security by design » et qu'ils sont vulnérables à l'usage intensif des clés USB pour migrer des données et installer des mises à jour logicielles.

Le rapport se garde bien de donner une piste sur les auteurs de cette cyberattaque. Mais des sources anonymes ont indiqué au *New York Times* que cette campagne a des similitudes avec d'autres attaques menées par un groupe connu sous le nom « *Energetic Bear* » qui serait lié à la Russie. Une hypothèse difficile à vérifier.

A lire aussi :

EDF produit le clone numérique de ses centrales nucléaires

Iliad va ouvrir un datacenter dans un abri antinucléaire

Photo credit: Let Ideas Compete via VisualHunt.com / CC BY-NC-ND