Comment des hackers ont provoqué une panne de courant en Ukraine

Publié il y a une dizaine de jours, un billet de blog du SANS ICS donne de nouveaux détails sur la panne dont ont été victimes plusieurs opérateurs de réseaux d'électricité en Ukraine, fin décembre. Le directeur de la branche spécialisée sur les systèmes industriels (Scada) du SANS, une organisation regroupant 165 000 professionnels de la sécurité, confirme que ce black-out a bien été provoqué par une attaque coordonnée et minutieusement préparée.

Mais, au-delà de cette affirmation qui étaye les premiers éléments publiés sur le sujet, le SANS livre une analyse en profondeur de l'attaque qui en dit long sur le degré de préparation des hackers. « *Cette attaque est composée d'au moins trois éléments : un malware, une attaque par déni de service sur le système téléphonique et une pièce manquante, qui renferme la cause réelle de l'impact (autrement dit ce qui a, directement, provoqué la panne de courant, NDLR)* », écrit Michael Assante, auteur du billet et directeur du SANS ICS. Selon ce dernier en effet, et contrairement à ce qu'avait suggéré l'éditeur Eset, ce n'est **pas le malware BlackEnergy et son module KillDisk**, retrouvés sur les réseaux des opérateurs piratés, qui sont à l'origine des coupures de courant, mais plutôt une intervention manuelle des hackers sur les systèmes Scada des stations de distribution d'électricité. Même si cette intervention a probablement été permise par l'infiltration du réseau des opérateurs via une opération de hameçonnage ciblée (spearphishing) visant à déployer un malware.

Ouverture des coupe-circuit, attaque du call center

Pour Michael Assange, une fois les réseaux corrompus, l'attaque coordonnée, qui a touché plusieurs opérateurs régionaux ukrainiens, s'est attachée, dans un premier temps, à rendre les opérateurs des réseaux de distribution d'électricité aveugles avant d'endommager les systèmes Scada à proprement parler, en ouvrant des coupe-circuit. En parallèle, un déni de service contre le call center des opérateurs empêchait les clients impactés de prévenir leur opérateur.

« *Deux théories se sont affrontées dans la communauté. Selon la première, le composant KillDisk était juste présent sur le réseau, sans lien avec la panne d'électricité. La seconde faisait de KillDisk le responsable direct du black-out. Nous pensons que ni l'une ni l'autre n'est juste* », écrit Michael Assante. Selon le SANS, un malware de type KillDisk n'aurait pas suffi seul à causer une panne, les systèmes industriels auraient en effet continué à fonctionner même après l'infection. « *Faire fonctionner un système électrique sans le bénéfice d'un système Scada au niveau de la distribution ajoute des risques, mais sans un changement d'état (par exemple une coupure d'alimentation), le système continue à opérer* », poursuit le directeur du SANS ICS. Bref, le malware utilisé par les hackers n'a été qu'**un facilitateur**, leur permettant de prendre pied sur le réseau et de préparer leur attaque.

Redémarrage en mode manuel

Même si le SANS précise qu'il ne possède pas de certitude absolue sur l'ensemble des éléments de cette trame, KillDisk avait aussi, selon lui, pour vocation de rendre les systèmes inopérants. Donc

de **retarder la restauration**, allongeant la durée de la panne, tout en complexifiant l'enquête sur l'origine de l'attaque. Cette tactique des hackers n'a toutefois pas fonctionné pleinement… Le SANS souligne en effet la réactivité « *impressionnante* » des opérateurs ukrainiens, qui sont repassés en mode manuel pour mettre fin à la panne. La reprise du service (qui a demandé entre 3 et 6 heures) s'est effectuée sans le bénéfice des systèmes de distribution Scada, alors toujours infectés. « *Des opérateurs qui reposent davantage sur l'automatisation pourraient ne pas être en mesure de restaurer de larges portions de leur système de cette façon* », prévient le SANS.

A lire aussi :

Panne de courant via une cyberattaque : les spécialistes ne sont pas surpris

Les 10 principales défaillances des systèmes Scada selon Lexsi

Crédit photo : chungking / Shutterstock