Comment une cyberattaque a mis des centrales ukrainiennes hors service

Comment une cyberattaque a mis des centrales ukrainiennes hors service ?

S'il reste encore des zones d'ombres, le doute n'est désormais plus permis : la panne électrique qui a touché l'Ukraine à Noël a bien été causée par une cyberattaque. C'est la première fois qu'un réseau électrique est mis hors service par une attaque informatique. Mais que les opérateurs d'importance critique soient prévenus : ce n'est sûrement pas la dernière.

Le rapport publié jeudi 3 mars par l'équipe de réponse d'urgence pour la sécurité informatique des systèmes de contrôle industriels (ICS-CERT) du département de la Sécurité intérieure des Etats-Unis (DHS) est sans appel : le blackout électrique qu'a connu une partie de l'Ukraine fin 2015 a bien été causé par des hackers. Il confirme ce faisant les conclusions avancées par le SANS ICS (un autre groupe d'experts en cybersécurité industrielle) début janvier, et entérine l'évènement comme étant la première attaque réussie sur un réseau électrique.

UNE SÉRIE D'ATTAQUES SOIGNEUSEMENT PLANIFIÉES

Les intrusions dans le réseau de trois opérateurs énergétiques ont impacté environ 225 000 clients. Bien que le service ait repris quelques jours plus tard, il reste encore limité, même à l'heure actuelle. D'après les témoins interrogés par l'ICS-CERT, les attaques auraient été coordonnées de telle manière qu'elles se sont produites à 30 minutes d'intervalle sur chaque réseau, touchant des installations centrales et régionales. L'opération a très probablement nécessité une longue reconnaissance et étude des victimes.

Lors de l'attaque, plusieurs individus ont pris l'accès des systèmes grâce à des outils de contrôle à distance, soit au niveau de l'OS, soit au niveau des systèmes ICS, le tout via des accès VPN (réseau privé virtuel) dont ils avaient précédemment obtenu les codes d'accès. Une fois l'attaque effectuée, le malware KillDisk a été utilisé pour effacer les fichiers compromis et corrompre les secteurs de démarrage des machines ou les firmwares des équipements pour les rendre inopérants. Les attaquants auraient également surchargé les centres d'appels des énergéticiens pour les empêcher de réagir immédiatement à l'évènement. De plus, trois autres organisations en charge d'infrastructures critiques ont aussi été pénétrées, mais sans impact direct sur leurs opérations.

DES ZONES D'OMBRES PERSISTENT

Malgré ces nouvelles informations, le rôle exact qu'a joué le malware BlackEnergy dans l'attaque n'est toujours pas connu. Ce malware, connu du milieu de la cybersécurité depuis 2007, a été retrouvé sur trois des systèmes impactés. Originellement présenté comme la potentielle arme du crime, il est possible qu'il n'ait en fait été utilisé que pour obtenir des codes d'accès. Il est aussi bon de noter que le rapport de l'ICS-CERT se base uniquement sur les témoignages du personnel IT de six organisations ukrainiennes qui ont été directement témoins des évènements, et pas sur une analyse technique du code ou du matériel impliqué dans l'incident.

Ces considérations mises à part, le fait que différents groupes d'experts soient d'accord sur l'origine cybercriminelle de la panne constitue une ultime (et sinistre) mise en garde à l'égard des opérateurs d'importance vitale (OIV). Car ces incidents ne font malheureusement que commencer. … [Lire la suite]

Réagissez à cet article

Source : *Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service*