Scada : quand une cyberattaque provoque une panne de courant

C'est un peu le scénario que redoutaient les experts. C'est aussi une première mondiale : un malware destructeur ayant infecté des autorités régionales de fourniture d'électricité en Ukraine a privé des centaines de milliers de foyers de courant **pendant quelques heures**, le 23 décembre dernier. L'agence de presse ukrainienne TSN expliquait, le lendemain, qu'environ la moitié des foyers de la région d'Ivano-Frankivsk (soit environ 1,4 million d'habitants) avait été privée d'électricité, en raison d'un malware qui déconnectait les sous-stations du réseau électrique.

Par la voix de son ministre de l'énergie, le gouvernement ukrainien a annoncé **l'ouverture d'une enquête** sur ces événements, les services secrets du pays pointant eux déjà la probable responsabilité de la Russie. L'Ukraine affirme avoir réussi à circonvenir l'attaque, limitant ainsi la durée de l'interruption de services.

Au début de cette semaine, les chercheurs en sécurité de la société spécialisée iSight Partners précisaient que la souche avait ciblé au moins trois opérateurs régionaux. Sur la base d'une analyse du malware, ils affirment que ce sont bien les dégâts provoqués par le virus qui ont conduit au blackout.

La porosité des systèmes Scada

De leur côté, les chercheurs d'Eset expliquent que la souche infectieuse ayant infecté les entreprises ukrainiennes dérive de BlackEnergy, malware découvert en 2007 et plusieurs fois mis à jour pour inclure des fonctions destructrices. Selon l'éditeur d'antivirus, les dernières versions de BlackEnergy incluent ainsi **un composant (KillDisk)**, chargé d'effacer des plages essentielles sur le disque dur des victimes afin notamment d'interdire le boot de l'OS, et semblent aussi s'être enrichies de fonctions permettant de saboter les systèmes chargés des contrôles industriels, les fameux Scada. Notamment en ciblant un processus gérant la connexion entre le port Ethernet et les ports série Eltima ou avec la plateforme ASEM Ubiquity (employée dans le contrôle industriel). S'y ajoute l'exploitation d'une backdoor dans un utilitaire SSH offrant un accès permanent aux assaillants. Selon Eset, les opérateurs régionaux ukrainiens ont été infectés via une macro piégée dans un document Microsoft Office, montrant une fois de plus la porosité entre l'informatique classique et des systèmes industriels de plus en plus connectés.

Le SANS Institute, une organisation regroupant 165 000 professionnels de la sécurité, a également analysé la souche infectieuse et parle d'un malware très modulaire. L'organisation estime, dans un billet datant du 1er janvier, qu'il est « *probable* » que la cyberattaque soit responsable du blackout. Probable mais pas encore établi à 100 %. « *Qui plus est, la fonction d'effacement du module (KillDisk, NDLR) vise probablement à effacer les traces des assaillants après l'attaque ; en elle-même, elle ne paraît pas être en mesure de provoquer la panne* », précise Robert Lee, l'auteur du billet de blog sur le SANS Institute et par ailleurs Pdg de Dragos Security.

« En mesure de provoquer la panne »

Dans son billet de blog, même s'il met en évidence des fonctionnalités de KillDisk semblant cibler des processus exploités pour le pilotage des Scada, Eset n'écarte pas que la panne ait pu être causée par des manipulations des assaillants via l'accès par backdoors. Mais les chercheurs de l'éditeur écrivent eux : « *notre analyse du malware destructeur KillDisk, détecté dans plusieurs compagnies de distribution d'électricité en Ukraine, indique qu'il est théoriquement en mesure de provoquer la panne de systèmes critiques* ».

BlackEnergy est tout sauf un inconnu, même si son objectif s'était jusqu'alors résumé à l'espionnage. En fin d'année dernière, en pleine campagne électorale dans le pays, il a ainsi infecté des médias ukrainiens, ce qui a conduit à la perte définitive de vidéos et autres contenus. En 2014, le groupe qui exploite ce malware, un groupe baptisé Sandworm par iSight, a ciblé l'OTAN, les gouvernements ukrainiens et polonais et des entreprises européennes sensibles, dont une société de télécommunications française dont le nom n'avait alors pas été précisé.

Après Stuxnet et Dragonfly

Ce n'est pas la première fois que des pirates ciblent le secteur de l'énergie. En juillet 2014, l'éditeur Symantec avait mis au jour un groupe d'assaillants, baptisé **Dragonfly**, qui était parvenu à pénétrer les systèmes d'entreprises de ce secteur, à des fins d'espionnage. Mais, selon Symantec, Dragonfly disposait aussi de moyens **«** *d'endommager ou d'interrompre la fourniture d'énergie dans les pays affectés* **»** via la corruption de systèmes. La France figurait alors au troisième rang des pays touchés par l'infection derrière l'Espagne et les États-Unis. L'éditeur américain expliquait alors que Dragonfly cachait très certainement un groupe de hackers bien financé et originaire de l'Est de l'Europe.

Rappelons que la première attaque informatique connue contre les Scada visait le programme nucléaire Iranien. Le virus Stuxnet, probablement développé par les États-Unis et Israël, avait alors détruit une bonne partie du parc de centrifugeuses utilisées par l'Iran dans le cadre de son programme d'enrichissement d'uranium. En décembre 2014, un rapport gouvernemental allemand révélait encore qu'un haut fourneau d'une aciérie du pays avait été endommagé suite à une attaque informatique.

A lire aussi :

Sécurité des Scada : pourquoi la côte d'alerte est atteinte

Thomas Houdy, Lexsi : « Après Dragonfly, réagir sur la sécurité des Scada »

Crédit photo : Menna / Shutterstock