Cyber-attaques : des centrales électriques en Ukraine prises pour cibles

Les centrales électriques de l'Ukraine visées par des attaques informatiques ? Un journal local (TSN) évoque ce scénario inquiétant.

Le 23 décembre dernier, la moitié de la zone d'Ivano-Frankivsk (ouest de l'Ukraine, 1,4 million d'habitants) se serait retrouvée sans électricité pendant quelques heures. 80 000 foyers auraient été affectés, précise Silicon.fr.

Récemment, les chercheurs de l'éditeur de solutions de sécurité d'origine slovaque ESET ont observé plusieurs attaques similaires visant des centrales électriques en Ukraine.

Les assaillants exploiteraient une famille de malware (BlackEnergy) afin d'introduire un logiciel malveillant (KillDisk) dans les systèmes informatiques.

Objectif tacite : saboter les ordinateurs d'exploitation des systèmes industriels (SCADA) des centrales électriques ou des compagnes d'électricité comme Prykarpattya Oblenergo.

Selon ESET, ce lien entre BlackEnergy (connu depuis plusieurs années) et KillDisk aurait été initalement détecté fin novembre par CERT-UA, la cellule nationale de sécurité informatique de l'Ukraine.

Le vecteur d'infection de BlackEnergy serait des fichiers Excel infectés (Microsoft Office) diffusés par des campagnes de phishing (hameçonnage) sur les ordinateurs en lien avec l'exploitation de systèmes industriels. Le tout parsemé d'une dose de social engineering (technique de manipulation).

Dans le scénario de Prykarpattya Oblenergo dans la région d'Ivano-Frankivsk, la panne serait survenue après "l'intervention de personnes non autorisées (…) dans le système de commande à distance" de la centrale électrique. Les techniciens ont dû rétablir le courant "manuellement", précise la compagnie locale d'électricité.

De son côté, Symantec considère que le malware "Disakil / KillDisk" a déjà été utilisé en octobre pour cibler des médias en Ukraine (il a notamment ravagé plusieurs ordinateurs d'un groupe média important du pays) et que le mode de contamination peut varier.

L'éditeur américain de solutions de sécurité précise que le groupe de pirate derrière ce cheval de Troie est connu sous le nom de Sandworm (exploitation de failles critiques Windows sous forme d'attaques zero day).

"Il a déjà frappé d'autres cibles comme l'OTAN, un certain nombre de pays d'Europe occidentale et des firmes du secteur de l'énergie", commente Symantec.

"Avec cette attaque et 5 ans après Stuxnet, on voit bien que la menace ciblant les systèmes industriels SCADA est plus que jamais présente et constitue un risque réel pour les infrastructures vitales d'un pays", commente Tewfik Megherbi, consultant avant-vente chez F5 Networks (fournisseur de solutions de load

balancing), dans une réaction envoyée à la presse spécialisée.

Pour sa part, Gérôme Billois, senior manager en gestion des risques et sécurité chez Solucom, commente sur Silicon.fr : *"Il faut rester prudent quant aux conclusions qu'on tire de l'affaire ukrainienne. On est ici dans un contexte où l'attribution est presque automatique (du fait du conflit entre l'Ukraine et la Russie, NDLR) et les informations disponibles émanent d'un nombre de sources limité. Si la panne de courant est toutefois bien due à une cyberattaque, cela ne constitue pas réellement une surprise."*

(Crédit photo : Shutterstock.com – Konstantin Romanov)