Malware et systèmes industriels : FireEye a détecté un TRITON ravageur

FireEye lance une alerte à propos de **TRITON**, un malware considéré comme une menace d'Etat compte tenu de ses capacités à infecter des systèmes critiques.

Il est susceptible d'infiltrer des réseaux d'infrastructures vitaux et de provoquer des dégâts majeurs en manipulant des configurations software de process industriels.

Dans une contribution blog en date du 14 décembre, l'éditeur américain de solutions de sécurité, spécialisé dans les détections précoces de menaces, fait le point sur TRITON. Tout en restant flou sur l'identification du groupe de hacking qui agit derrière ou sur les assauts déjà repérés.

Mais FireEye est persuadé que ce groupe agit pour le compte d'un Etat.

« Le fait de cibler des infrastructures critiques pour couper, dégrader ou détruire des systèmes est cohérent avec les attaques nombreuses et les tentatives de reconnaissance furtive réalisées par des Etats comme la Russie, l'Iran, la Corée du Nord, les Etats-Unis et Israël », selon les chercheurs de l'éditeur.

« Les intrusions de ce type ne constituent pas forcément un indice d'une volonté imminente de couper les systèmes visés mais peuvent représenter un signal pour une éventuelle attaque. »

Outre FireEye, Symantec s'est également intéressé à ce malware Triton (lire le focus en anglais).

Le cas de Stuxnet en 2010 a marqué l'histoire de la sécurité IT. Ce virus, développé par les Etats-Unis et Israël, avait endommagé les centrifugeuses d'enrichissement d'uranium de la centrale de Natanz exploitées dans le cadre du programme nucléaire iranien.

D'autres assauts visant des infrastructures vitales de pays ont été détectés : l'attaque Shamoon, attribuée à l'Iran, a visé en 2012 des systèmes informatiques du groupe pétrolier saoudien Saudi Aramco.

En 2016, une centrale électrique avait été visé par un malware en Ukraine. L'assaut, a priori d'origine russe, avait entraîné une coupure de courant gigantesque (250 000 foyers affectés), rappelle Silicon.co.uk.

(Crédit photo : Shutterstock.com)