Panne électrique en Ukraine : le malware aurait été aidé par l’humain

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

Le mois dernier, une cyberattaque contre des fournisseurs d'énergie ukrainiens avait privé 80 000 clients d'électricité. D'après la signature du malware, l'attaque avait été imputée à un groupe de pirates ayant des liens avec la Russie. Mais, selon une nouvelle étude, le malware n'est pas directement à l'origine de la panne : les assaillants sont intervenus physiquement pour activer les disjoncteurs et provoquer la coupure de courant.

Selon des informations publiées samedi par l'équipe du SANS Industrial Control Systems (ICS), une organisation spécialisée dans l'information et la formation des professionnels de la sécurité, le malware a bien servi aux pirates à s'introduire dans le réseau des fournisseurs d'électricité, mais ils sont ensuite intervenus sur les disjoncteurs pour couper l'alimentation. Depuis des années, les experts mettent en garde sur la vulnérabilité des systèmes de contrôle industriels. Les cyberattaques survenues le 23 décembre contre les installations ukrainiennes montrent que leurs craintes sont justifiées. Selon les experts du #SANS ICS, ces évènements sont aussi la preuve que de telles attaques sont planifiées et très coordonnées.
Depuis l'annexion de la Crimée par la Russie en 2014, les tensions entre la fédération et l'Ukraine restent fortes. « Pour masquer le piratage et l'intrusion dans les réseaux, les agresseurs sont intervenus physiquement sur la centrale électrique », a déclaré l'équipe du SANS ICS. « Les agresseurs ont également lancé en simultané une attaque DDoS par déni de service sur le réseau téléphonique afin de bloquer les appels des clients affectés par la panne », a encore déclaré l'organisation. Les attaques auraient visé les deux fournisseurs d'énergie Prykarpattyaoblenergo et Kyivoblenergo. Ce dernier a déclaré dans une mise à jour de service que 80 000 clients dépendant de 30 sous-stations avaient été déconnectés du réseau.

Des pannes provoquées par une action physique

Plusieurs entreprises de sécurité ont analysé le #malware Black Energy 3 et le #composant Killdisk utilisés pour les attaques. Jeudi dernier, l'entreprise de sécurité iSight Partners basée à Dallas a déclaré que ces logiciels malveillants avaient déjà été utilisés dans le passé par le #groupe de pirates Sandworm connu pour avoir de puissants intérêts russes. Mais, comme iSight, le SANS ICS pense que les pannes ne sont pas à mettre exclusivement sur le compte des malwares. « Autrement dit, de nouvelles preuves pourraient remettre en cause l'impact réel des composantes malveillantes impliquées dans l'attaque », a écrit Michael Assante, directeur du SANS ICS.
Le composant Killdisk écrase le Master Boot Record (MBR), premier secteur du disque dur chargé par le PC avant de monter le système d'exploitation, et empêche donc le PC de démarrer. Selon Symantec, Killdisk peut aussi écraser des fichiers en écrivant des données inutiles. Michael Assante avance que Killdisk n'était pas compatible avec le système SCADA de contrôle et d'acquisition de données utilisé par les deux opérateurs. Mais il a peut-être été utilisé pour effacer d'autres fichiers qui auraient permis la restauration des systèmes. « Il semble que les fournisseurs d'électricité ont rétabli leurs services en actionnant manuellement les disjoncteurs au bout de trois et six heures », a ajouté le directeur du SANS ICS. Selon lui, « il faudrait féliciter les opérateurs ukrainiens pour leur diligence et les efforts accomplis pour restaurer leurs services ».

Réagissez à cet article

Source : *Panne électrique en Ukraine : le malware n'est pas seul en cause – Le Monde Informatique*