Cyberattaques en Ukraine : après l'électricité, l'aéroport de Kiev

Rebelote ? En tout cas, ce lundi matin, le centre de réponse aux incidents cyber ukrainiens (le CERT-UA) prévient les entreprises locales de la menace que fait peser une vague de cyberattaques sur le pays. Après une intrusion qui a ciblé plusieurs opérateurs régionaux d'électricité et a provoqué une panne d'électricité pour environ 80 000 foyers, c'est **l'aéroport principal de Kiev** qui serait la cible des assaillants. Au cours du week-end, un malware a été retrouvé sur les systèmes informatiques de Boryspil, le principal aéroport du pays qui concentre environ 60 % du trafic aérien international de l'Ukraine.

Reuters explique que le virus présent sur cette installation critique pour le pays pourrait être proche de celui retrouvé chez les entreprises de distribution d'électricité Prykarpattyaoblenergo et Kyivoblenergo. Rappelons que l'attaque contre ces deux entreprises utilisait notamment une APT (Advanced Persistent Threat ou menace persistante avancée) de la famille **BlackEnergy**. Pour l'heure, il est trop tôt pour savoir s'il s'agit là d'une attaque de grande ampleur visant à mettre à mal les installations aéroportuaires ; le service de presse de Boryspil parlant pour l'instant d'une seule station de travail infectée. Une source militaire ukrainienne explique à Reuters que l'infection a été détectée très tôt et qu'elle n'a causé aucun dommage.

Moscou pointé du doigt

Sur son site, le CERT-UA publie une liste d'indicateurs de compromission relatifs à BlackEnergy et invite les administrateurs systèmes à vérifier leurs logs à la recherche de ces indices. Le centre de recherche renvoie également vers un article de *SecureList* (animé par Kaspersky) détaillant les caractéristiques de BlackEnergy. « *Ces assaillants prennent la peine de se dissimuler et de préserver leur présence à long terme au sein des environnements compromis* », écrivaient en novembre 2014 Maria Garnaeva et Kurt Baumgartner. Bref, toutes les caractéristiques de l'APT. Déjà en 2014, les chercheurs notaient la volonté des concepteurs de BlackEnergy de **cibler de nouveaux environnements**, dont les systèmes industriels Scada.

Très rapidement après la panne des opérateurs d'électricité fin décembre, les services secrets ukrainiens ont pointé la responsabilité de leurs homologues russes, sans toutefois étayer leurs accusations. Une société américaine, iSight, rappelle, elle, que l'utilisation de BlackEnergy est associée à un **groupe de hackers russes appelé Sandworm**. Un groupe qui a déjà ciblé des installations Scada en Europe et aux Etats-Unis et qui « *opère en alignement avec les intérêts de l'Etat (russe, NDLR)* », selon John Hultquist, de iSight. Ce lundi, une source officielle russe pointe le fait que le malware mise au jour à l'aéroport de Kiev est lié à un serveur de commande et contrôle situé en Russie.

A lire aussi :

Panne de courant via une cyberattaque : les spécialistes ne sont pas surpris

Les 10 principales défaillances des systèmes Scada selon Lexsi

Crédit photo : Dmitry Birin / Shutterstock