Un malware soupconné d’être à l’origine d’une coupure de courant en Ukraine

Un malware soupconné d’être à l’origine d’une coupure de courant en Ukraine

Le 23 décembre, les habitants de la ville ukrainienne d'Ivano-Frankivsk ont subi une importante panne de courant. Celle-ci a été provoquée par une défaillance provenant de la centrale électrique régionale et a affecté plusieurs milliers de foyers de la région. Mais cette soudaine panne n'était pas un accident : en effet, la société chargée de l'exploitation de la centrale a précisé que celle-ci avait été causée par des « interférences » sur leurs systèmes.

Mais pour plusieurs médias locaux, la piste d'une cyberattaque visant les infrastructures énergétiques du pays est à privilégier. La société de cybersécurité ESET a d'ailleurs publié plusieurs informations en ce sens : la société explique avoir récupéré des samples de malware ayant affecté plusieurs centrales ukrainiennes, et explique que ceux-ci ont pu être utilisés dans le cadre d'une cyberattaque à l'encontre des équipements ukrainiens.

Des nouvelles du cyberfront

ESET se dit en mesure d'affirmer que plusieurs entreprises Ukrainiennes du secteur de l'énergie sont victimes de cyberattaques. Les attaquants ont notamment recours à une famille de malware baptisées BlackEnergy, dont les traces ont été détectées à plusieurs reprises en 2015 dans des entreprises ukrainiennes liées au secteur de l'énergie.
BlackEnergy est un malware connu, qui a déjà été repéré plusieurs fois par le passé. Celui-ci se présente sous la forme d'un malware modulaire : une fois la cible infectée, les attaquants peuvent exploiter la porte dérobée ainsi créée afin de télécharger des modules différents permettant au malware d'accomplir diverses actions sur la machine cible.
Parmi les modules identifiés de ce malware, l'un d'entre eux permet notamment de s'attaquer aux systèmes SCADA, des postes utilisés pour le contrôle et la surveillance des installations industrielles. BlackEnergy permet également le téléchargement d'un autre malware, baptisé cette fois killdisk, et dont l'objectif est la destruction de données. Un arsenal qui laisse ESET penser que ces outils ont pu être mis en œuvre dans l'attaque dont semble avoir été victime la centrale électrique d'Ivano-Franivsk.
Les services de sécurité ukrainiens accusent la Russie d'être à l'origine de l'attaque selon Reuters, mais ces derniers n'ont émis aucun commentaire venant confirmer ou infirmer cette théorie. Une enquête a été ouverte par les autorités nationales pour déterminer les circonstances exactes de cette coupure de courant.

Réagissez à cet article

Source : *Ukraine : un malware soupconné d'être à l'origine d'une coupure de courant*