CybercriminalitÃ© : Faut-il payer?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 3/2/2023 14:00:00

Le 25 janvier dernier, quatre Ã©tablissements au sein du Groupe Ramsay SantÃ© ont Ã©tÃ© ciblÃ©s par des hackers. A ce jour, aucune donnÃ©e nâ□□a Ã©tÃ© dÃ©robÃ©e et lâ□□impact sur les patients reste mineur.

En 2019 dÃ©jÃ , le groupe Ramsay avait Ã©tÃ© la cible dâ□□une cyberattaque dont l'ampleur avait eu d'importantes rÃ©percussions sur le fonctionnement des Ã©tablissements touchÃ©s pendant plusieurs semaines.

Dans un contexte oÃ¹ les cyberattaques contre des Ã©tablissements de santÃ© se sont multipliÃ©es ces derniers mois, Fabien Rech, Senior VP EMEA de Trellix - leader dans le domaine de la cybersÃ©curitÃ© - rappelle que :

Pendant longtemps, de nombreux acteurs de la menace avaient pour rÃ¨gle tacite de ne pas s'attaquer aux hÃ´pitaux. Les tensions gÃ©opolitiques qui dÃ©coulent du conflit russo-ukrainien semblent toutefois indiquer qu'ils on Ã©tÃ© remis sur la liste des cibles, ce qui pourrait expliquer le pic d'activitÃ©s observÃ© ces derniers mois.

Les hÃ´pitaux sont des cibles particuliÃ¨rement allÃ©chantes pour les pirates informatiques car ils disposent de systÃ¨mes informatiques complexes et rarement sÃ©curisÃ©s grÃ¢ce Ã la technologie XDR. Dans la plupart des cas, la technique d'attaque utilisÃ©e est celle du ranÃ§ongiciel.

A la question de s'il faut ou non payer la ranÃ§on, la rÃ©ponse peut dans certains cas s'avÃ©rer positive, en particulier si des donnÃ©es hautement sensibles sont en jeu, mais cela a un coÃ»t.

Les consÃ©quences financiÃ¨res sont importantes et il existe un risque rÃ©el que lâ□□Ã©tablissement concernÃ© ne reÃ§oive pas ses donnÃ©es dÃ©cryptÃ©es en retour, ou soit confrontÃ© Ã des demandes rÃ©pÃ©tÃ©es de ranÃ§ongiciels par la suite. S'appuyer sur l'intÃ©gritÃ© des acteurs de la menace est un risque que les Ã©tablissements de santÃ© ne peuvent tout simplement pas se permettre de prendre.