Hôpitaux : une cible privilégiée des cyberattaques au rançongiciel

La multiplication des attaques informatiques à destination des hôpitaux en France et dans le monde inquiète. Ces établissements de santé sont devenues une cible évidente pour des cybercriminels en quête de rançon.

Il y a une semaine, l'hôpital de Dax a été paralysé par une cyberattaque au rançongiciel, qui bloquait toutes les données de son réseau contre le paiement d'une rançon. Quelques jours plus tard, c'est au tour du centre hospitalier de Villefranche-sur-Saône de faire les frais du même type d'attaque informatique. Un phénomène qui n'est pas nouveau puisque cela est déjà arrivé aux 6 000 ordinateurs du CHU du Rouen en novembre 2019. Certains cybercriminels ont, depuis, profité du Covid-19 pour multiplier les actions sur ces établissements de santé.

Les cyberattaques contre les hôpitaux ont bondi de 500% en un an dans le monde, selon le cabinet de conseil PwC. En cause? Sa grande surface d'attaque et la présence de données sensibles. Une opportunité rêvée pour les cybercriminels. Mais, interrogé par Maddyness, Baptiste Robert, chercheur en cybersécurité et hacker éthique – alias Elliot Alderson sur Twitter -, tient pourtant à nuancer le phénomène : « *Il n'existe pas de méchants à capuche qui ciblent les hôpitaux parce que ce sont des hôpitaux. Ces lieux sont des victimes privilégiées pour les cybercriminels car, quand ils découvrent une*

faille sur un réseau de centaines de machines – que ce soit M6, le concepteur de jeux vidéo CD Projekt ou l'hôpital de Dax -, ils y voient une opportunité de rançon élevée » .

À lire aussi

Hôpitaux intelligents : le défi de la sécurité informatique

En effet, la plupart des cybercriminels scannent l'intégralité d'internet et testent toutes les failles de sécurité sur les systèmes ouverts et à disposition, sans cible précise. « *95% du temps, leur mode opératoire consiste à tester de vieilles failles connues pour s'infiltrer, infecter tout un réseau, chiffrer le contenu des ordinateurs pour les rendre inopérants et afficher une note de rançon contre lesquels ils rendraient leur butin* » , précise l'expert.

« Arrêtons de payer les rançons »

Alors pourquoi les attaques au rançongiciel contre les hôpitaux explosent en ce moment ? « *Ces endroits sont une ville dans la ville. Beaucoup de métiers, d'informations sensibles, de niveaux techniques et de postes connectés s'y trouvent. C'est un grand réseau qui regorge de données critiques. Il est donc dur d'en faire l'inventaire précis et de savoir combien de machines sont connectées à internet, sachant que la pompe à oxygène de la chambre 5 par exemple peut en faire partie ! »* , insiste Baptiste Robert. Autant de portes d'entrées potentielles pour les attaquants informatiques qui, par la nature des données qu'ils détiennent, pensent pouvoir faire plier plus facilement les institutions.

Pour sortir de ce cercle vicieux, le chercheur en appelle à arrêter de payer les rançons.

« Aujourd'hui les attaques au ransomware explosent pour la simple et bonne raison que ça fonctionne, les victimes paient une fois sur deux en moyenne.

C’est une aubaine pour les cybercriminels » , détaille-t-il.

Trois précautions peuvent aussi être mises en place pour éviter au maximum d’être ciblé :

faire l’inventaire de toutes les machines connectées à son réseau;

s’assurer qu’elles soient régulièrement mises à jour;

faire des sauvegardes très souvent à l’extérieur de son réseau.

Il faut également savoir comment réagir dans l’immédiat suite à une attaque potentielle, intégrer des réflexes simples comme appeler la gendarmerie ou débrancher les ordinateurs. Mais, pour se prémunir des attaques, « *pas de recette magique* » selon le hacker. « *Ces situations exigent d’agir rapidement et, l’administration française étant très lente, avec beaucoup de paperasse, cela rend les process souvent très compliqués »,* déplore Baptiste Robert.

Article écrit par HELOÏSE PONS