Un hôpital paye la rançon mais n’obtient rien en échange.

	Un hôpital paye la rançon mais n’obtient rien en échange

Certains groupes de pirates qui exploitent des ransomwares pour faire fortune sans effort n'ont ni morale ni parole, si l'on en croit la prise en otage de données d'un hôpital, qui a payé pour rien la rançon demandée.

Les maître-chanteurs sont aussi parfois de véritables escrocs, et ça n'est jamais une bonne idée de céder à leurs exigences. Après la messagerie chiffrée Protonmail qui avait payé une rançon et avait malgré tout continué à subir des attaques DDOS massives, c'est un hôpital américain qui l'apprend à ses dépens.

Ainsi Network World rapporte que le Kansas Heart Hospital à Wichita a accepté de payer une rançon après que des pirates ont réussi à infecter son système informatique avec un ransomware, qui chiffre les données stockées avec une clé que seul le ravisseur connaît. Ce n'est pas le premier hôpital à être visé et à céder ainsi à un chantage informatisé, mais c'est la première fois que les pirates ne respectent pas leur part du marché. Pire, ils en demandent plus.

PAYER ENCORE POUR DÉBLOQUER UN PEU PLUS

L'attaque avait eu lieu la semaine dernière, et avait rendu des fichiers de l'hôpital inaccessibles, sans possibilité de recourir à des archives. Pour les débloquer, il fallait payer de l'argent en utilisant un service anonymisé, sur Tor, avec un compte en bitcoins intraçable. Étant donnée l'importance des données, les administrateurs de l'établissement ont accepté de payer une somme indéterminée, relativement faible. Mais plutôt que de déchiffrer les données, les pirates n'en ont libéré qu'une petite partie, et exigé davantage d'argent pour déchiffrer le reste.

L'hôpital a alors refusé. « Ce n'était plus une manœuvre sage ou une stratégie », s'est justifiée la direction, qui a mis en place un plan B pour limiter les effets de l'attaque. Selon le Kansas Heart Hospital, aucun patient n'a eu à subir d'effets négatifs en raison de l'indisponibilité de certaines données… [Lire la suite]

Réagissez à cet article

Source : *Ransomware : un hôpital paye la rançon mais n'obtient rien en échange – Business – Numerama*

Auteur : Guillaume Champeau