

# Ransomware : un hôpital US paye pour retrouver son réseau

Le Hollywood Presbyterian Medical Center est devenu un établissement de santé très médiatique. Pas nécessairement pour ses compétences médicales, mais plutôt pour sa faiblesse en matière de sécurité informatique. En effet, en début de semaine, on apprenait que [l'hôpital avait été victime d'un ransomware](#), bloquant une bonne partie du système d'information. Selon les informations de la presse américaine, le cybercriminel demandait 9000 bitcoins, ce qui représente à peu près 3,2 millions d'euros pour un retour à la normale.

Après quelques jours d'incertitudes et d'emballement médiatique, le responsable du centre médical, Allen Stefanek, est sorti de son silence pour donner quelques détails. Le plus important est qu'il a été obligé de payer une rançon pour reprendre le contrôle des PC. Mais les sommes annoncées ne sont pas mirobolantes, le dirigeant explique qu'il a versé « 40 bitcoins soit l'équivalent de 17 000 dollars (15 000 euros) ». Il justifie ce paiement comme étant, « *la façon la plus rapide et la plus efficace pour restaurer notre système et les fonctions administratives* ». Aucun détail n'a été fourni sur le niveau réel de cette attaque, mais Allen Stefanek assure « *les soins des patients n'ont pas été affectés, ni les dossiers des patients* ».

## Les entreprises n'hésitent plus à payer

Pour autant, des mesures de sécurité ont été prises pour palier le blocage du système. Les urgences ont été redirigées vers un autre hôpital, le personnel de santé redécouvre les

crayons et le papier pour enregistrer les informations patients et le fax pour communiquer avec les autorités. L'attaque a eu lieu le 5 février dernier, mais la direction de l'hôpital a attendu la semaine dernière pour informer la police de Los Angeles du problème. Le FBI est aussi de la partie en prenant en charge l'enquête. A noter que la rançon a été payée avant que les autorités judiciaires soient sollicitées.

Cette attaque apporte plusieurs enseignements. Le premier est la montée en puissance inexorable des rançongiciels. Les cybercriminels redoublent de sophistication, allant de la programmation ([JavaScript](#)) ou de [l'intégration du service client avec un chat](#). La création d'un ransomware est [un investissement très lucratif](#). Surtout que les entreprises n'hésitent pas à payer pour déverrouiller les PC infectés. Une étude de Skyhigh montre que près d'un quart des entreprises sont prêtes à payer une rançon et 15% seraient capables d'y mettre 1 millions de dollars. La nouvelle plaie de la sécurité pourrait être combattue, mais cette bataille nécessite [une politique un peu plus volontariste des autorités](#).

**A lire aussi :**

[Les implants médicaux, prochaines cibles des ransomwares](#)

[Un ransomware change le code PIN des terminaux Android](#)

**Crédit Photo : Epstock-Shutterstock**