Une rançon après la cyberattaque au CHU de Rouen ? Ce que réclament les pirates

By Rédaction Normandie

Published: 2019-11-19 · Archived: 2026-04-06 00:06:11 UTC

Le CHU de Rouen a été victime d'une cyberattaque, vendredi 15 novembre 2019. Depuis, les pirates réclament de l'argent pour libérer des fichiers infectés. Explications.

Le centre hospitalier universitaire de Rouen (Seine-Maritime) a été touché par une cyberattaque, vendredi 15 novembre 2019. (©Raphaël Tual/76actu/archives)

Par **Rédaction Normandie** Publié le 19 nov. 2019 à 12h24

La grande **cyberattaque** qui a touché les sites du **centre hospitalier universitaire (CHU)** de **Rouen (Seine-Maritime)**, vendredi 15 novembre 2019, laisse encore des traces quatre jours après son déclenchement.

Outre la mise au ralenti du système informatique de l'établissement durant le week-end, certains services ont découvert, lundi 18 novembre 2019, une impossibilité d'accéder aux ordinateurs comme à certains fichiers hébergés sur les différents serveurs internes. Le cryptovirus, entré sur tous les postes allumés à 19h45 vendredi, aurait aussi corrompu certains stockages externes. Et pour cause : catégorisé *ransonware* (ou rançongiciel, en français), ce dernier exige désormais à quiconque tente de contacter les pirates une somme d'argent pour libérer les accès.

De nombreux fichiers verrouillés

Si les services du CHU ont globalement pu reprendre leur activité, notamment dans le cadre des soins aux patients, d'autres s'échinent à remettre la main sur des documents de travail nécessaires à certaines activités de soins, de recherche, d'organisation, d'agenda…

Selon une source interne contactée par *76actu*, de nombreux fichiers (Excel, Word, .doc…) sont bel et bien verrouillés par les pirates informatiques. Ces derniers sont cryptés sous le suffixe .clop, et génèrent spontanément un message texte que nous avons pu consulter.

« Tous les fichiers de chaque serveur du réseau ont été encryptés à l'aide d'un algorithme puissant », peut-on d'abord lire.

> Tout le réseau est bloqué, ne débloquer qu'un seul ordinateur est impossible.

Des consignes pour ne pas corrompre les fichiers cryptés sont fournies, et deux adresses e-mail (hébergées .su, pour Soviet Union…) sont associées. Elles sont adressées au « CEO » (le directeur général de l'entreprise, en anglais). Avec une précision, propre au *ransonware* : « Nous n'avons pas besoin de vos fichiers et de vos informations. »

Payer ? « Inimaginable », pour l'hôpital

Nous avons également pu consulter le mail automatiquement généré lorsque l'on adresse un message aux contacts figurant sur le message. Il y est question d'une demande d'argent pour débloquer la situation. Celle-ci s'élève à 40 bitcoins, soit l'équivalent de 300 000 euros, selon le cours numérique actuel de la cryptomonnaie.

« On n'a pas reçu de réelle demande de rançon, directement et formellement adressée à l'hôpital », nuance la communication de l'établissement. En effet, le message réclamant 40 bitcoins n'est en fait qu'une réponse type, ne mentionnant pas l'hôpital, mais automatiquement envoyée à quiconque joint les pirates par voie électronique. L'établissement pourrait-il accepter de payer pour récupérer ses données ? « Inimaginable », pour l'hôpital.

> Il a été évoqué que si jamais nous devions être rançonnés un jour, on ne paierait pas, indique le service communication.

La structure préfère s'en remettre aux sept experts de l'Agence nationale de la sécurité informatique (ANSI), d'ores et déjà venus prêter main forte aux 30 personnels informatiques de l'établissement. Leur mission : déverrouiller les algorithmes bloquants. Une tâche ardue, dont l'issue ne sera pas assurément heureuse : « Au contraire, on pense que ça peut être très difficile de débloquer. On réinitialise depuis jeudi. »

> Si l'ANSI ne trouve pas la clé de déchiffrement, il y aura probablement des gens qui vont perdre leurs fichiers.

Une enquête pour extorsion en cours

Du reste, toujours selon la communication de l'établissement, « étant donné le nombre d'applications possédées par le CHU », il faudra « au moins la semaine » avant de retrouver une situation normale. Là non plus, « on ne peut le garantir », souligne le service.

A l'heure actuelle, d'anciennes sauvegardes sont restaurées et un mode dégradé opère provisoirement au sein des ordinateurs vérolés.

Par ailleurs, une plainte a été déposée en fin de matinée, lundi 18 novembre. Samedi, le Parquet de Paris, compétent en matière de cybercriminalité, avait déjà ouvert une enquête pour « extorsion et tentative d'extorsion en bande organisée », notamment. Mis à l'arrêt numérique dès vendredi par le cryptovirus, l'établissement rouennais avait dû « revenir vingt ans en arrière et repasser à la bonne vieille méthode du papier et du crayon » afin d'assurer son activité principale : l'accueil des patients.

En parallèle, la direction appelle à ne pas saturer les urgences :
La désorganisation provoquée par la cyberattaque dont a été victime l'hôpital n'aide pas à la fluidité du service d'urgences. La faute au retour de certaines procédures de format papier, et à la durée rallongée des prises en charge. Ainsi, la direction appelle à solliciter en priorité son médecin généraliste, avant d'envisager un séjour inévitable aux urgences.
