

Des hackers attaquent l'AP-HP en pleine crise du coronavirus

L'attaque informatique a, dimanche, bloqué brièvement les accès à Internet des établissements de santé parisiens.



Illustration. Des pirates informatiques ont tenté de paralyser l'informatique centrale de l'AP-HP. LP/Olivier Boitet

Par Damien Licata Caruso

Le 23 mars 2020 à 19h44

Dès janvier, Guillaume Poupard, patron de l'Agence nationale de la sécurité des systèmes d'information (Anssi), le prophétisait : « Les attaquants n'ont pas d'éthique donc ils seraient capables d'attaquer les CHU au moment d'une crise quand nous avons besoin d'eux pour [être sûr de récupérer une rançon](#) ».

C'est arrivé : dimanche, l'Assistance publique-Hôpitaux de Paris, qui gère 39 hôpitaux publics en Île-de-France, a été victime d'une brève mais intense attaque informatique. [Confirmant une information de L'Express](#), l'AP-HP a annoncé avoir subi en fin de matinée, sur deux de ses adresses Internet, une attaque par déni de service ou « DDoS ».

Ce piratage consiste à générer une grande quantité de connexions simultanées afin de surcharger les serveurs. Cette cyberattaque, qui a duré une heure, « a été gérée par le prestataire de l'AP-HP et n'a jamais atteint ses infrastructures », a précisé l'Agence. Mais cette manœuvre éclair pourrait ne pas être l'objectif final des attaquants.

Une tentative venue de loin

« Ce type d'attaque peut permettre de saturer les systèmes de sécurité afin de placer une éventuelle attaque plus intelligente qui donnerait accès plus tard au système complet et préparer l'installation d'un rançongiciel », analyse Arnaud Lemaire, directeur technique de F5 Networks, une entreprise de cybersécurité spécialisée dans la protection contre les attaques « DDoS ».

Durant l'attaque, ce prestataire privé a décidé de diminuer les accès Internet « pour gérer au mieux la situation », ce qui a eu pour conséquence de bloquer l'accès externe à la messagerie, à Skype ainsi que l'accès externe aux applications de l'AP-HP.

« Ils essayent de faire mal une fois et peuvent demander un paiement sous peine de recommencer de manière plus violente. Comme une forme de terrorisme », assure Arnaud Lemaire de F5 Networks.

Newsletter L'essentiel du matin

Un tour de l'actualité pour commencer la journée



[S'inscrire à la newsletter](#)

[Toutes les newsletters](#)

Comme souvent, il est quasiment impossible d'attribuer cet acte de piraterie à un groupe de hackers ou à un pays. Élément troublant, toutefois, l'attaque a été jugulée et la situation est revenue à la normale quand les accès hors Europe ont été bloqués...

Dans la rubrique High-tech

[Australie : une loi oblige désormais les géants de la tech à rémunérer les médias](#)

[Facebook va investir 1 milliard de dollars dans les contenus d'actualité en 3 ans](#)

Abonnés [Ziwit, une entreprise de Montpellier, protège gratuitement les CHU contre les](#)

[hackers](#)

 [VOIR LES COMMENTAIRES](#)

High-tech

Australie : une loi oblige désormais les géants de la tech à rémunérer les médias

Abonnés **Ziwit, une entreprise de Montpellier, protège gratuitement les CHU contre les hackers**

Abonnés **E-commerce : un Français sur deux utilise son smartphone pour faire du shopping**

Abonnés **«Les plates-formes de travail numérique doivent respecter le cadre européen»**