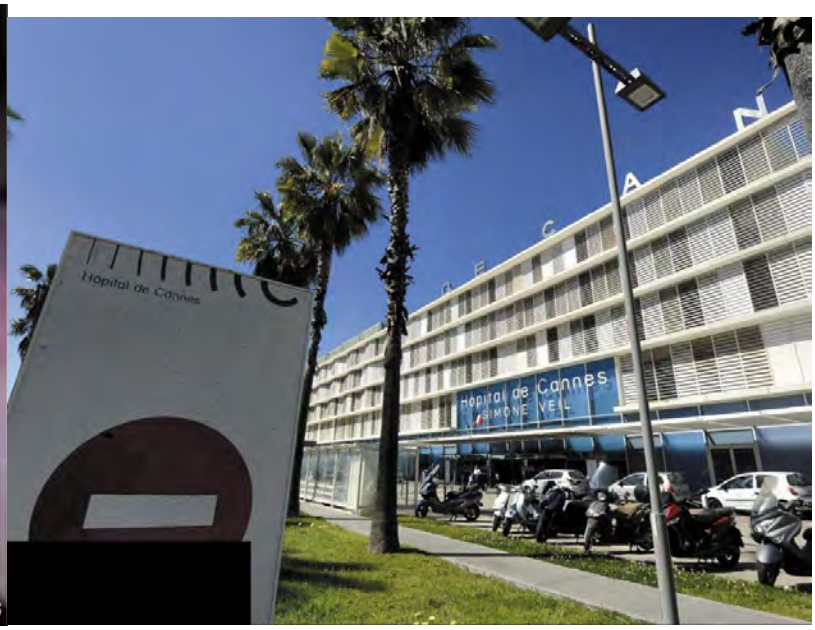
Pour l'établissement Simone-Veil à Cannes, victime d'une cyber-attaque, l'ultimatum a expiré. Que va-t-il se passer si la rançon exigée n'est pas versée ? PAGES 2 ET 3



Cyberattaque à l'hôpital : une rançon, sinon quoi ?

Après le « black-out » informatique provoqué par une cyberattaque sur l'hôpital de Cannes le 16 avril, une demande de rançon lui a été adressée ce mardi 30 avril. Elle a expiré la nuit dernière...

Les hackers ne connaissent pas de trêve pour le 1er mai. Pour le groupe de pirates informatique Lockbit 3.0., pas question de stopper un *« travail illégal »*, une activité criminelle, qui peut éventuellement rapporter gros, après avoir semé le chaos.

Quinze jours après une cyberattaque sur l'hôpital Simone-Veil de Cannes, qui a provoqué la paralysie complète de son système informatique, une demande de rançon lui a été adressé, a révélé l'établissement ce mardi 30 avril.

Pour l'heure, le montant réclamé n'est pas connu. Mais le délai de versement a expiré la nuit dernière à minuit. Pour quelles conséquences ?

« Les établissements publics de santé ne paient jamais de rançon face à ce type d'attaque », exclut d'emblée le CHU de Cannes.

Quid d'éventuelles données confidentielles, qui pourraient être livrées en pâture par les hackers de Lockbit 3.0. ? *« Nous communiquerons à nos patients et à nos parties prenantes, au terme de l'examen détaillé des fichiers ayant pu être exfiltrés, sur la nature des informations dérobées. »*

En attendant, les investigations techniques des gendarmes experts en cybersécurité – du Centre de lutte contre les criminalités numériques C3N saisi de l'enquête, dont l'antenne régionale est située à Marseille – se poursuivent, tandis qu'une plainte a été déposée.

« Un tiers de l'activité a dû être décalé »

« L'adresse du serveur pirate est située aux États-Unis, mais ça ne signifie évidemment pas que l'Amérique nous a attaqués ! », précisait également Yves Servant, directeur de l'hôpital Simone-Veil, lors d'une précédente interview.

Pour parer à la cyberattaque le 16 avril dernier, une cellule de crise avait décidé de mettre à l'arrêt tout le système informatique – 350 serveurs, pour 1 500 postes de travail –, après alerte de l'Agence Nationale de Sécurité dès 6 h 30 du matin.

Un « black-out » qui avait obligé l'hôpital à reporter toutes les opérations et consultations non urgentes dans un premier temps, avant de poursuivre son activité en *« mode dégradé »*, c'est-à-dire en utilisant des formulaires papier lorsque cela est possible.

« Environ un tiers de notre activité globale a dû être décalé, sachant que nous effectuons environ 6 500 interventions chirurgicales par an », estimait encore le directeur de Simone-Veil.

Pour absorber ce déficit, la solidarité départementale a joué avec les hôpitaux de Nice – notamment pour l'expertise informatique –, d'Antibes et Grasse pour la prise en charge rapide de nouveaux patients cannois, *« dont certains ont été détournés via le Samu.*

« On verra l'étendue des dégâts... »

« Aujourd'hui, on peut prendre un rendez-vous pour une intervention planifiée, mais on doit garder un équilibre entre le maintien d'une activité hospitalière et la bonne sécurité de nos patients. »

Si les urgences sont toujours restées ouvertes, le retour à la normale est annoncé très *« progressif et minutieux »*, au fur et à mesure de la remise en service des logiciels, dans un ordre évidemment prioritaire.

On demande donc aux patients de faire preuve de… patience.

Mais du point de vue du personnel, dès le lendemain de la cyberattaque, on s'inquiétait déjà de l'après, *« lorsqu'on verra l'étendue des dégâts. Qu'est ce qui a été volé ? Les identités des patients, les numéros de sécurité sociale, nos RIB, nos fiches de paie, qu'est-ce qu'on va récupérer ?*, s'interrogeait une employée de Simone-Veil. *Tout ce qui aura été fait sur papier en attendant que ça ne reparte va devoir être intégré dans le dossier de chaque patient. C'est là qu'il faudra faire attention à ne pas faire d'erreur. »*

Quoi qu'il en soit, cette piraterie marquera durablement les esprits, même si l'hôpital cannois s'y était préparé. Avec ce constat d'une autre salariée : *« Cette situation, c'est du jamais vu depuis trente ans ! »*

ALEXANDRE CARINI
acarini@nicematin.fr

Les différentes attaques dans la région

Des services de la Corsica Ferries aux casinos varois en passant par la Chambre de commerce et d'industrie Nice Côte d'Azur, les hackers ciblent à tout va. Tour d'horizon.

27 octobre 2023 : le site de la Corsica Ferries à l'arrêt : les réservations en ligne auront été inaccessibles pendant près de 24 heures.

Nuit du 30 au 31 août 2023 : le système informatique de la CCI coupé après une attaque

19 avril 2023 : onze établissements du groupe Vikings Casinos, dont ceux de Sanary et Fréjus dans le Var, ont été fermés après une cyberattaque de type « rançongiciel ». Les deux établissements ont pu rouvrir leurs portes en deux temps, fin avril et début mai 2023.

Nuit du 9 au 10 novembre 2022 : le Conseil départemental des Alpes-Maritimes repère une cyberattaque. Une plainte a été déposée. Le Département a assuré ne pas avoir cédé à la demande des pirates qui ont mis à exécution leur menace.

15 décembre 2022 : le CHU de Nice, selon *Le JDD*, fait l'objet d'une cyberattaque mais les outils – le pare-feu (firewall) – mis en place ont été efficaces : *« Le pare-feu du système informatique a bien fonctionné empêchant toute intrusion dans le serveur de la messagerie de l'établissement. Mais nous restons vigilants »*, indiquait alors le CHU. Le 19 avril 2021, le CHU avait déjà été victime d'une *« défaillance au niveau de l'infrastructure réseau »*. La direction du centre hospitalier avait réfuté la thèse d'une cyberattaque. Ordinateurs, téléphonie : plus rien ne fonctionnait.

P. P.

Interview express

Pascal Le Digol, expert en cybersécurité

« Les pirates ont déjà gagné »


(DR)

Pour Pascal Le Digol, expert en cybersécurité, responsable France de WatchGuard technologies, éditeur de solutions de cybersécurité, la partie est déjà gagnée pour les hackers qui ont attaqué l'hôpital Simone-Veil de Cannes.

Qu'est-ce que cette cyberattaque de l'hôpital de Cannes dit de la vulnérabilité du système informatique de nos hôpitaux ?
La même chose que les fois d'avant, comme à Corbeil-Essonnes. C'est récurrent. Ce sont des systèmes qui ont des surfaces d'attaque colossales. C'est un système d'information énorme, très ouvert, dont le matériel informatique n'est potentiellement pas mis à jour. Ou qui utilise des logiciels qui ont été développés dans un but médical et pas forcément dans une visée de sécurité informatique totale. C'est un terrain de jeu facile pour les pirates. C'est la même chose dans les communautés de communes, il y a plein de logiciels, dont certains développés maison.

Comment s'en prémunir ?
Les techniques de protection, on les connaît ; ça demande de l'humain, du temps, du budget, ce n'est pas forcément ce que les hôpitaux ont le plus en rab' actuellement. Il faut un calendrier sur plusieurs années pour arriver à un bon niveau de sécurité, sachant qu'en France on a un retard et un niveau de déficit sur cet aspect sécurité informatique.

Le groupe Lockbit a posé un ultimatum. Qu'ont à craindre les hôpitaux et les patients si la rançon n'est pas payée ?
N'importe quelle donnée peut être utilisée pour attaquer une personne. En général, ils les revendent. Les pirates qui ont attaqué l'hôpital de Cannes ont déjà gagné. Ils n'ont pas la rançon ? Pas grave. Ces données ont une valeur sur le marché noir ; ça se revend à d'autres groupes de pirates qui vont faire des campagnes de phishing. Si vous recevez un email avec au début votre numéro de sécurité sociale et des infos sur vous, c'est forcément plus crédible que quelque chose de générique qu'on va mettre en spam. Et là, ces informations sont plus que sensibles, car seuls quelques organismes les connaissent.

Que pouvez-vous dire de LockBit, qui est derrière ce hacking ?
C'est une revendication du groupe, mais est-ce que ce sont eux ? Ou une fausse revendication ? On a déjà vu de fausses revendications. Ce qui est sûr c'est que LockBit, qui a fait l'objet d'une vaste opération internationale pour le mettre à terre, en février dernier, impliquant dix pays, a besoin de montrer qu'il est encore en vie. C'est comme une hydre à plusieurs têtes qui repoussent quand on en coupe une. Ils ont identifié les vulnérabilités qui ont conduit aux arrestations, les ont comblées. Ça fait peur. S'ils sont revenus sur le devant de la scène, avec des infrastructures renforcées, il y a de quoi s'inquiéter.

Les hôpitaux ne payent vraiment jamais ?
C'est une directive de l'État français de ne pas payer. Officiellement en tout cas. Après, je ne sais pas. En tant que citoyen, je me demande si des données médicales importantes, critiques, sont perdues. Si oui, ne pas les récupérer est dangereux. S'il y a des sauvegardes, il n'y a aucune raison de payer. La seule raison qui pousserait à payer, c'est s'il y a des données médicales ultrasensibles perdues.

RECUEILLI PAR G. L.

« Urgence cyber » : un numéro vert

Le conseil régional de Provence-Alpes-Côte d'Azur a ouvert le 17 avril dernier un centre Urgence Cyber à Toulon (Var) pour accompagner les établissements victimes d'attaques. Il concerne les entreprises de la région. L'idée est simple : en appelant un numéro d'urgence, l'entreprise, collectivité ou association victime d'une attaque cyber obtient un diagnostic gratuit de la situation.

Il permet ensuite la mise en place d'un plan de sauvetage, en s'appuyant sur des partenaires – une cinquantaine au total — locaux, moyennant des tarifs très accessibles. Le but est de restaurer l'activité de la victime et surtout de sauvegarder ses données.

Le centre Urgence Cyber est joignable sur simple appel au 0 805 036 083 ou via son site internet.

Qui est LockBit, ce groupe de hackers ?

« Notre travail ne s'arrête pas ici. LockBit pourrait essayer de reconstruire son entreprise criminelle ». Les craintes de Graeme Biggar, directeur général de la NCA, l'Agence de lutte contre la criminalité britannique, n'étaient pas infondées. Le 20 février dernier, le groupe de cybercriminels LockBit, présenté comme *« le plus nuisible »* au monde, a été démantelé. Son site internet et ses serveurs ont été bloqués.

De retour aux affaires ?

Mais le répit a été de courte durée. Sur les sites spécialisés, le nom de ce cybergang a très vite refait surface. Pour certains, il s'agissait d'entretenir l'illusion de continuité de ses activités. La cyberattaque dont a été victime l'hôpital Simone-Veil de Cannes, le 16 avril, pourrait prouver le contraire. Pour SaxX, hacker « éthique » et chercheur en cybersécurité, ils sont *« repartis de plus belle »*.
Dans un long communiqué du 30 avril, l'établissement cannois annonce avoir fait l'objet d'une demande de rançon venant de LockBit 3.0, avec un ultimatum fixé à la nuit dernière, à minuit. Ce piratage avait entraîné des annulations d'opérations et de consultations au sein de l'établissement. Pascal Le Digol, expert en cybersécurité et responsable France de WatchGuard Technologies, prend des pincettes : *« Est-ce que ce sont eux ? Ou est-ce une fausse revendication ? C'est à vérifier. On a déjà vu de fausses revendications. Ce qui est sûr, c'est que LockBit a besoin de montrer qu'ils sont encore en vie. »*
« C'est plus qu'une vraie revendication », assure SaxX. *« Il n'y a pas de doute. Elle est affichée sur le site, sur un mur de la honte, avec les autres prises de guerre. C'est même à prendre un peu trop au sérieux »*. Et de souligner *« la résilience assez folle »* du groupe de hackers. En atteste, avec ce compte à rebours qui devrait passer au vert à minuit cette nuit, un échantillon de données pourrait être mis en ligne…

Une méthode éprouvée

Une chose est certaine. La méthode qui a affecté le bon fonctionnement de l'hôpital azuréen reste la même depuis 2019, quand le groupe a été repéré pour la première fois. Le modus operandi est éprouvé : bloquer des données et exiger une rançon pour les débloquer. En cas de refus, les données sont diffusées et, à terme, revendues sur le dark web.
Cependant, plutôt que d'opérer lui-même une gigantesque opération criminelle, LockBit met son logiciel malveillant *[LockBit 3.0, ndlr]* à la disposition de ses affiliés – des pirates indépendants – qui lui versent ensuite un pourcentage des rançons obtenues : ça s'appelle du « rançongiciel à la demande » ou « Raas », pour « Ransomware as a Service » en anglais. *« Derrière Lockbit, il y a des Russes, mais pas seulement »*, précise Pascal Le Digol. *« Les affiliés peuvent être partout dans le monde, y compris en France, en Belgique »*, abonde SaxX.

La barrière éthique vole en éclats

En quelques années d'activités, LockBit et ses affiliés ont causé des milliards de dollars de dégâts et extorqué des dizaines de millions de dollars de rançons à leurs victimes, rappelle le hackeur éthique. Des banques, des services postaux ou des hôpitaux figurent parmi leurs cibles.
En France, LockBit a été à l'origine de 27 % des demandes de rançons en 2022 et 2023. *« LockBit est un groupe de pirates qui à la base se refusaient à attaquer les hôpitaux »*, indique Le Digol. *« Ils avaient même remboursé un hôpital qui s'était fait attaquer par des affiliés. On ne peut pas parler d'éthique pour un cybergang mais ils s'étaient mis cette limite. »*
Pour Pascal Le Digol, le fait qu'une de leurs premières grandes victimes, à leur retour, soit un hôpital, est *« un signe fort en termes de communication. Cela veut dire : "Vous avez essayé de nous faire tomber, on va taper partout où on peut désormais". »*
Une manière aussi de montrer, comme le décrypte SaxX, *« qu'il ne se sont pas fait ridiculiser »* lors de l'opération de fin février. *« Ils veulent regagner la confiance de leurs affiliés. Sans eux, ils ne sont rien »*.

PIERRE PEYRET
ppeyret@nicematin.fr

Cyberattaque : quelles sont les données dérobées à l'hôpital ?

Des milliers de documents, volés à l'issue de la cyberattaque du groupe de hackers Lockbit contre l'hôpital de Cannes le 16 avril, ont été publiés sur le darkweb. Pour quelle utilisation ?

« *Là débute une nouvelle crise, on entre dans une nouvelle phase d'un point de vue cybercriminel.* » Voici comment le hacker éthique et chercheur en cybersécurité SaxX qualifie la suite logique de la cyberattaque (nos éditions d'hier). Les 61 gigas de données personnelles piratées et volées, désormais disponibles sur le darkweb, vont être consultés, disséquées, triées, réorganisées... et revendues. « *On retrouve bilan de santé, évaluation pédiatrique, psychologique… En gros, de nombreuses informations critiques sur les patients de l'hôpital de Cannes. Les données de tout le personnel aussi y figurent... carte d'identité, RIB, bulletin de salaire, infos personnelles* », a révélé hier SaxX sur X (ex Twitter).

« Petites mains » à l'œuvre

Le hackeur éthique, qui a pu consulter une partie des données piratées, a pris le soin de dissimuler les informations sensibles des clients et personnels de l'hôpital.

Mais c'est là où réside tout l'intérêt des « petites mains » désormais à l'œuvre pour revendre et faire circuler ces données : ces dernières vont pouvoir revendre des lots d'informations qui peuvent s'avérer très intéressantes, à plusieurs niveaux.

« *Imaginez que demain, un des membres de votre famille, qui est passé par le CHU de Cannes, veuille contracter un prêt. Moi demain, je suis assureur, je vais avoir accès directement à ces informations-là.* »

Des informations personnelles qui vont directement pouvoir influer sur la décision de la banque. « *Aujourd'hui, il existe un véritable marché parallèle sur lequel les données concernant l'état de santé et la solvabilité des gens sont achetées par des banquiers, des assureurs* », continue SaxX.

Mais ce n'est pas tout. « *Demain, je vous appelle et me fais passer pour votre banquier en vous donnant ces infos-là : je vous dis qu'on va procéder à une réévaluation de votre taux et vous allez renseigner d'autres infos beaucoup plus personnelles, car vous vous sentirez totalement en confiance. C'est là où c'est totalement insidieux.* »

Phishing ciblé

Les données personnelles divulguées vont aussi permettre des campagnes de phishing (hameçonnage) géolocalisées et très ciblées. Ces dernières suivent généralement des calendriers bien établis, comme avec les aides de la CAF, ou bien lors d'événements de plus grande envergure, tels que les Jeux olympiques ou les élections européennes. Les utilisateurs ciblés trouvent alors logique de recevoir un e-mail qui « colle » à la temporalité de l'événement.

Plus près de chez nous, il y a le Festival de Cannes. « *Pourquoi ne pas envoyer un message aux Cannois pour leur proposer de gagner une place à une projection spéciale. Vous êtes Cannois, c'est un euro, foncez, il n'y a que 10 places disponibles* », imagine encore le hackeur SaxX.

Et il faut alors renseigner vos coordonnées bancaires, etc. C'est l'engrenage.

MARGOT MENTHA

« Une plainte déposée »

Dans un communiqué, la direction de l'hôpital « *condamne cette publication et regrette les dommages éventuellement occasionnés auprès de ses patients, professionnels et partenaires. Un retour circonstancié et personnalisé sera réalisé auprès des personnes et institutions concernées* ».

Tandis qu'un service spécialisé en cybercriminalité de la gendarmerie poursuit ses investigations, l'hôpital confirme qu' « *une plainte a été déposée* ». La CNIL (Commission nationale de l'informatique et des libertés) et l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ont également été alertés.

Malgré le black-out informatique provoqué par cette cyberattaque, l'hôpital précise encore que son « *activité a repris son cours quasi ordinaire. Le rétablissement du fonctionnement normal de son système d'information se fait à un rythme soutenu...* »

Les opérations et consultations non urgentes avaient été annulées le jour même, et l'hôpital avait fonctionné uniquement avec des formulaires papier lorsque c'était possible. « *Environ un tiers de l'activité globale avait dû être décalé* », a reconnu le directeur Yves Servant.

A. C.