# Face à la multiplication des attaques, la Fra

*Le gouvernement va investir un milliard d'euros supplémentaire d'ici à 2025 pour faire monter le niveau généra*

INGRID VERGARA @Vergara_i

**CYBERCRIMINALITÉ** La liste des hôpitaux, collectivités territoriales et entreprises françaises victimes de cyberattaques s'allonge désormais quotidiennement. En 2020, la cybercriminalité a été multipliée par quatre par rapport à l'année précédente, si l'on s'en tient aux nombres d'interventions de l'Agence nationale de sécurité des systèmes d'information (Anssi), chargée de la protection cyber de l'État. La crise sanitaire n'a certes rien arrangé, mais elle n'est pas à l'origine de cette accélération. Tous les pays et tous les secteurs d'activité y sont confrontés, pour la simple raison que des criminels ont trouvé depuis des années dans l'espace cyber un moyen relativement peu coûteux mais en revanche très lucratif d'exercer des activités illégales. Avec des méthodes d'attaques désormais industrialisées, souvent sophistiquées, parfois appuyées par des considérations géopolitiques, ils frappent à tout va, profitant de la fragilité d'entreprises, d'établissements de santé, de collectivités, d'associations ou de simples particuliers bien démunis. Avec de lourdes conséquences opérationnelles et économiques pour toutes les victimes.

**255 %**
L'augmentation des interventions de l'ANSSI sur des attaques entre 2019 (54 opérations) et 2020 (192 opérations)

Pour répondre à la croissance exponentielle de ces menaces sérieuses, l'État français a donc décidé d'accélérer sa stratégie de cyberdéfense. Présentée jeudi par le président Emmanuel Macron, elle vise à relever le niveau général de protection des acteurs publics et privés ainsi qu'à donner un coup d'accélérateur au développement de la filière de la cybersécurité en France.

### Muscler la détection

Dans le cadre du plan de relance et du programme d'investissement d'avenir, la France va investir un milliard d'euros supplémentaires d'ici à 2025 dans cette stratégie nationale. Ils viendront s'ajouter à des financements déjà prévus pour l'aide à la transition numérique des administrations. Des moyens supplémentaires (136 millions d'euros) vont être alloués à l'Anssi pour réaliser notamment des diagnostics de sécurité auprès des établissements de santé et des collectivités territoriales, en s'appuyant sur des acteurs locaux de confiance. Des solutions seront testées sur des sites pilotes (un territoire, un hôpital) et répliqué ensuite à l'échelle nationale. L'Anssi veut aussi renforcer les moyens de détection des attaques, en créant des CERT (Computer Emergency Response Team) régionaux, autrement dit des structures capables de réagir efficacement en cas d'urgence et d'assister les victimes.

Pour développer ses capacités de protection, la France mise aussi sur le développement de solutions technologiques de pointe. Cinq cents millions d'euros y seront consacrés, par le financement de projets de centres de recherche (Inria,CNRS, CEA…) ou


**HÔPITAL DE VILLEFRANCHE-SUR-SAÔNE** Le réseau informatique de l'hôpital Nord-Ouest a été attaqué lundi 15 février. Des opérations ont été reportées mais aucun transfert de patients n'est programmé.

**RABOT DUTILLEUL** L'entreprise de BTP a été attaquée en juillet 2020. Elle a mis 6 semaines pour retrouver 90 % de ses applications. Elle a pu récupérer l'intégralité de ses données.

**20 %**
des entreprises en France déclarent avoir subi une attaque au rançongiciel en 2020
*(source: Baromètre Cesin)*

**3 à 7**
semaines
Le temps pour se remettre d'une cyberattaque, selon la taille de l'entreprise, son niveau de résilience et le type d'incident
*(source: Wavestone)*

## Rabot Dutilleul: « Une cyberattaque est très anxiogène pour toute l'entreprise »

Rares sont les entreprises qui acceptent de témoigner après une cyberattaque. La société de BTP Rabot Dutilleul en a fait la douloureuse expérience en juillet 2020. Son directeur informatique raconte.

*« Nous avons un gros problème ».* Ce mardi matin de juillet 2020, François Depoortere, directeur informatique de Rabot Dutilleul, comprend rapidement, après lecture des rapports informatiques de la nuit, que le système d'information est victime d'une attaque au rançongiciel. *« Vous tentez d'ouvrir des fichiers, ils sont cryptés. L'activité est bloquée. Puis, dans un fichier, les pirates se présentent, exigent une rançon en bitcoins en échange de la clé de cryptage, dont le montant doublera tous les sept jours si vous n'y répondez pas. Ils menacent aussi de rendre publiques des données qu'ils affirment avoir captées. »* Le dirigeant du groupe est aussitôt prévenu et une cellule de crise mise en place. Première action prise pour circonscrire le risque: couper les systèmes. *« À ce moment-là, vous ne savez pas encore qui vous attaque, comment ils sont entrés, ni s'ils sont encore là »*, raconte François Depoortere. Autre priorité: prévenir les collaborateurs. Comment, sans aucun accès informatique? *« La chaîne de SMS marche très bien dans ce cas. Nous avions la liste de tous les téléphones pour leur dire en direct de ne plus toucher à rien. »* Tous les sites français du groupe, basé dans le Nord et qui emploie 1 500 personnes, sont concernés.

Commence alors une course contre la montre. *« Tout le jeu est de remonter le système le plus vite possible avec le moins d'impact possible sur l'activité de l'entreprise »*, résume François Depoortere. La cellule de crise définit chaque jour les priorités et les actions à mener pour pouvoir redémarrer l'activité opérationnelle. *« Nous n'avions pas encore de plan de reprise d'activité établi. Nous avions prévu de le faire au dernier trimestre de l'année. Heureusement, j'avais les réflexes d'une précédente expérience professionnelle. Si vous avez les processus majeurs de l'entreprise en tête, vous pouvez les prioriser quelle que soit l'entreprise dans laquelle vous travaillez »*, se souvient le responsable informatique.

> « Cette gestion de crise nous a coûté quelques ulcères à l'estomac »
> FRANÇOIS DEPOORTERE

Les deux activités principales de l'entreprise – la construction et la promotion – ne sont pas impactées avec la même force. *« Sur les chantiers, vous pouvez encore aujourd'hui vivre quelques jours sans informatique. En revanche, pour la vente aux particuliers, il y a eu un vrai coup d'arrêt »*, se rappelle François Depoortere. Heureusement, l'attaque est survenue en juillet, un mois traditionnellement plus calme pour l'activité.

La cellule de crise coordonne la communication interne et externe. Il faut prévenir les clients, les fournisseurs, etc. Après 48 heures, la messagerie est rétablie. *« Une cyberattaque est un événement très anxiogène pour les collaborateurs d'une entreprise. Il faut les rassurer. C'est un véritable exercice de communication d'entreprise. »* Cette communication se fait dans un premier temps via des groupes WhatsApp, pour partager des décisions prises ou remonter des questions, puis l'entreprise met en place un wiki et un chat pour une communication claire et efficace. Anxiogène, la situation l'est aussi pour l'équipe informatique en première ligne tant que la certitude que les attaquants ne sont plus là ou qu'ils ont pas laissé d'autres pièges n'est pas acquise. Cela prendra deux semaines. *« On a dessiné les scénarios catastrophe. Il y a eu un instant la crainte de ne pas pouvoir redémarrer certaines applications critiques, comme le paiement des fournisseurs, dans une période de crise du Covid très délicate. Si vous ne pouvez plus payer, vous ne pouvez plus produire et là, vous êtes mort. »*

Dans le cadre d'une cyberassurance souscrite par le groupe, l'entreprise se fait accompagner par un cabinet pour contrer l'attaque et l'aider à reconstruire le système d'information. Au bout de six semaines, l'entreprise parvient à remonter 90 % de ses applications. Elle a pu récupérer l'intégralité de ses données et reprendre enfin une activité normale. *« Cette gestion de crise nous a coûté quelques ulcères à l'estomac, mais elle a été très formatrice. L'entreprise a eu une bonne réponse collective et a fait un grand bond en avant sur la sécurisation des systèmes d'information, en termes d'outils, de processus et de formation des collaborateurs. »* Un conseil à partager après cette expérience ? *« Préparer un scénario pour fonctionner sans système d'information, avoir des PC en dehors de l'entreprise et les téléphones de tous les collaborateurs ainsi qu'une liste des tâches à effectuer en priorité pour pouvoir redémarrer au plus vite l'activité. »* ■ I. V.

## Une épidémie d'attaques au ranç

JEAN CHICHIZOLA
jchichizola@lefigaro.fr

Plongés dans le combat contre la pandémie… et attaqués par des cybercriminels. Après Marmande le 30 juin 2020 ou encore Albertville le 21 décembre dernier, les centres hospitaliers de Dax et de Villefranche-sur-Saône viennent d'être infectés par un rançongiciel. Ces logiciels malveillants, dont l'hôpital de Rouen avait déjà été victime en novembre 2019, bloquent les systèmes informatiques. Et les malfaiteurs proposent ensuite de « libérer » l'accès et les données contre une rançon. Au besoin, les cybervoyous utilisent d'autres logiciels comme à Narbonne le 10 décembre où l'hôpital fut attaqué par un virus visant à créer de la cryptomonnaie. En 2020, selon le secrétaire d'État à la transition numérique Cédric O, vingt-sept cyberattaques majeures, tous virus informatiques confondus, ont visé des hôpitaux.

Au total, l'Agence nationale de la sécurité des systèmes d'information (Anssi, rattachée au Secrétaire général de la défense et de la sécurité nationale) recense actuellement une tentative d'attaque par semaine sur des infrastructures comme des Ehpad (maisons de retraite médicalisées), Centres hospitaliers universitaires, hôpitaux, cliniques ou d'autres entités en lien avec des services de santé. Dans la plupart des cas, il s'agit de rançongiciels. Dans son récent rapport, disponible sur internet, sur « l'État de la menace rançongiciel », l'Anssi souligne que, à l'échelle mondiale, *« les hôpitaux et autres entités du secteur de la santé représentent globalement l'une des cibles privilégiées des attaquants »*, une tendance *« accrue en 2020, notamment dans le contexte de pandémie liée au Covid-19, l'attaque poussant sans doute plus facilement les hôpitaux à payer la rançon au vu du besoin critique de continuité »*. Tous secteurs d'activité confondus, et en incluant donc la Santé, un rançongiciel aurait rapporté, de mars à juillet 2020, 25 millions de dollars aux malfaiteurs. Un autre aurait généré 150 millions de dollars de « recettes » depuis son lancement en 2018. Concernant spécifiquement le monde de la Santé, les spécialistes observent que dans certains cas, les assaillants savent visiblement qu'ils ont touché une infrastructure de ce secteur alors que, dans d'autres cas, ils ne semblent pas avoir conscience de leur cible.

Pour les victimes, le résultat est bien sûr le même. Ainsi au centre hospitalier de Villefranche-sur-

# nce accélère sa stratégie de cybersécurité

*l de protection et accélérer le développement de la filière industrielle française dans ce domaine stratégique.*

par des projets collaboratifs avec des sociétés privées. Seules des technologies de pointe pourront, par exemple, aider des PME à automatiser la sécurité de leur système d'information, sécuriser efficacement des objets connectés ou adresser les problèmes spécifiques de certains secteurs.

Pour l'État, il s'agit aussi d'un enjeu de développement économique et de souveraineté majeur. D'ici à 2025, il souhaite multiplier par quatre le chiffre d'affaires de la filière (pour atteindre 25 milliards d'euros) et doubler le nombre d'emplois créés. Le secteur de la cybersécurité souffre d'une pénurie de profils et d'un manque certain d'attractivité, notamment auprès des filles. Pour y remédier, la stratégie met aussi l'accent sur la formation. Une fois les besoins prioritaires recensés, de nouvelles formations et de nouveaux masters seront créés et financés.

Enfin, l'État investit aussi dans le « campus cyber », pour renforcer les liens entre tous les acteurs français de la cybersécurité. En septembre 2021, cet immeuble de treize étages, dans le quartier de la Défense, près de Paris, réunira au sein d'un même lieu la crème du savoir-faire, privé et public : des grandes entreprises (Orange CyberDefense, Atos, Capgemini, Airbus Defence&Space, Sopra Steria..), des PME, des start-up, des administrations, des laboratoires de recherche et d'innovation, des centres de formation, etc. L'objectif est de renforcer à la fois les capacités de veille, de détection et de réponse aux menaces partagées, en développant par exemple une base de données commune.

> **« Tout le monde à un rôle à jouer »**
> L'AGENCE NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Parallèlement, sur les terrains policier et judiciaire, la France va continuer et intensifier sa stratégie de coopération européenne et internationale pour tenter de démanteler les réseaux cybercriminels, souvent réfugiés dans des zones de non-droit. De récents succès ont permis de mettre à terre Emotet, une gigantesque infrastructure qui a rançonné des centaines de milliers d'internautes pendant des années, ou encore d'arrêter plusieurs pirates du groupe Egregor.

Si cela redonne le moral aux défenseurs, cette difficile poursuite des attaquants ne suffit pas. « *Ce qui cassera la courbe exponentielle des attaques, c'est promouvoir une prévention efficace à chaque niveau. Tout le monde à un rôle à jouer* », martèle-t-on à l'Anssi. Selon le dernier baromètre du Cesin, l'association des responsables de la sécurité informatique, pour 80 % des entreprises ayant déclaré avoir connu une attaque en 2020, le vecteur d'entrée a été le phishing (un mail avec un lien malveillant sur lequel un collaborateur a cliqué). Pour rappeler à tout le monde les gestes barrières essentiels en matière d'hygiène informatique, la plateforme de référence cybermalveillance.gouv.fr fera aussi l'objet d'une campagne de promotion dans les prochains mois. ■


VILLE D'ANGERS, L.OUVIER (SABELLE/PHOTOPQR/SUD OUEST/MAXPPP. ERIC LE BRUN / LIGHT MOTIV. RICHARD MOUILLAUD/PHOTOPQR/LE PROGRES/MAXPPP

**HÔPITAL DE DAX**
Victime d'une attaque au rançongiciel dans la nuit du 8 au 9 février, l'hôpital de Dax est toujours sans système d'informatique. Des soins ont été reportés ou annulés. Aucun rendez vous ne peut être pris.

**MAIRIE D'ANGERS**
Une cyberattaque a visé mi janvier le système d'information de la ville et de la métropole. Les usagers n'ont pas pu accéder aux services en ligne de la ville.

**80 %**
**des entreprises**
ayant subi une attaque en 2020 déclarent que l'hameçonnage (phishing en anglais) a été le premier vecteur d'intrusion
*(source : Cesin)*

## ongiciel touche les hôpitaux français

Saône, le 15 février, où une attaque a été détectée à 4 h 30 du matin. Le rançongiciel concerné, Ryuk, celui-là même qui a rapporté 150 millions de dollars depuis 2018, est déjà une vieille connaissance des spécialistes en France et ailleurs dans le monde (on estimait en octobre 2020, qu'il était responsable de 75 % des attaques sur le secteur de la santé aux États-Unis, qu'il attaquerait depuis le premier semestre 2019). Ce 15 février, dans le Rhône, trois sites sont impactés : Villefranche-sur-Saône, Tarare et Trévoux. Pour limiter les dégâts, on coupe en urgence les accès du système informatique à internet, on déconnecte les postes de travail à l'exception des urgences. Le téléphone est aux abonnés absents. On peut imaginer le stress dans un quotidien où chaque seconde compte, déjà marqué par la fatigue et la lutte pour la vie. Comme ce fut le cas dans les autres attaques, le pire a été évité mais une série de mesures, classiques en la matière, ont dû être prises : orientation des urgences vers d'autres établissements, report temporaire d'interventions chirurgicales. Et il faut ensuite réparer les machines tout en continuant à soigner les êtres humains.

### Chaque attaque met potentiellement en danger la vie des patients

Ainsi à Dax, où le directeur par intérim du centre hospitalier attaqué le 9 février observait que l'agression, « *massive par son ampleur, a des conséquences sur tout le système médical, financier, de communication* ». Pour un temps, on en revient au papier, aux tableaux et aux photocopies. Quiconque a été privé un jour de sa carte Vitale aura une petite idée du problème. Sans oublier bien sûr la nécessité de mettre à jour les fichiers des patients. À chaque attaque, la priorité absolue, et toujours respectée, est de préserver au maximum l'activité médicale. Un objectif encore compliqué quand, ce qui est le cas la plupart du temps, plusieurs sites sont touchés en même temps. Comme à Albertville le 21 décembre avec deux sites hospitaliers, des Ehpad et des unités de soin de longue durée. Et il est évident que chacune de ces attaques met potentiellement en danger la vie des patients.

Pour faire face à l'augmentation de cette menace, un travail sur la sécurisation du secteur de la santé a été lancé par l'Anssi et les acteurs de la santé fin 2019, avant le début de la crise sanitaire. Cent quinze établissements de santé ont d'ores et déjà réalisé un diagnostic de leur niveau de sécurité (sur les parties les plus critiques du système d'information) via les outils proposés par l'Agence. Une dizaine d'établissements sont suivis au quotidien dans des travaux de sécurisation plus approfondis.

Mais les cybercriminels ne restent pas inactifs. Tous secteurs économiques confondus, les attaques par rançongiciels traités par l'Anssi (une partie seulement de ces attaques dont certaines demeurent inconnues) sont passées de 54 en 2019 à 192 en 2020. La seule véritable riposte est, au-delà de la réparation des dégâts, de porter plainte, comme les hôpitaux visés l'ont fait. Cédric O a souligné l'arrestation la semaine dernière de pirates informatiques suspectés d'être en rapport avec un rançongiciel « *grâce à une coopération entre les services français, les justices françaises et américaines, et nos partenaires européens* ». Mais, dans de trop nombreux cas, les cibles acceptent de payer la rançon, souvent après proposition d'un rabais par les maîtres chanteurs. ■

## À Angers, des dégâts pour la ville et ses habitants

Comme de très nombreuses collectivités locales françaises ces derniers mois, la mairie d'Angers et la communauté urbaine Angers Loire Métropole ont été victimes d'une cyberattaque. Dans la nuit du 15 au 16 janvier, des attaquants bloquent le système d'information. « *Le site internet, celui des bibliothèques, les logiciels, les ordinateurs... Tout était hors-service* », raconte un élu. Les serveurs sont rapidement coupés pour éviter une propagation de l'attaque dans le système. « *Le diagnostic a conclu à une attaque de type rançongiciel qui a frappé La Rochelle, Aix Marseille, Vincennes, l'Ademe... dans un passé récent* », explique la métropole dans un post Facebook, pour informer ses habitants.

La cyberattaque a des conséquences immédiates sur la vie des administrés. Fermeture des bibliothèques municipales faute de pouvoir accéder aux bases de données, impossibilité de délivrer un certificat de naissance ou d'effectuer des démarches relatives aux titres d'identité, toutes les bornes de service à l'accueil de la mairie inutilisables...

### Retour au papier

À l'intérieur de la mairie, la vie aussi se complique pour les agents qui doivent réapprendre à vivre sans ordinateurs. Documents, applications, messageries, accès internet... Rien ne leur est accessible. La collectivité utilise habituellement 200 logiciels métiers. Le vieux fax au sous-sol reprend du service, notamment pour envoyer le dépôt de plainte au procureur et un signalement à la Commission nationale de l'informatique et des libertés (Cnil).

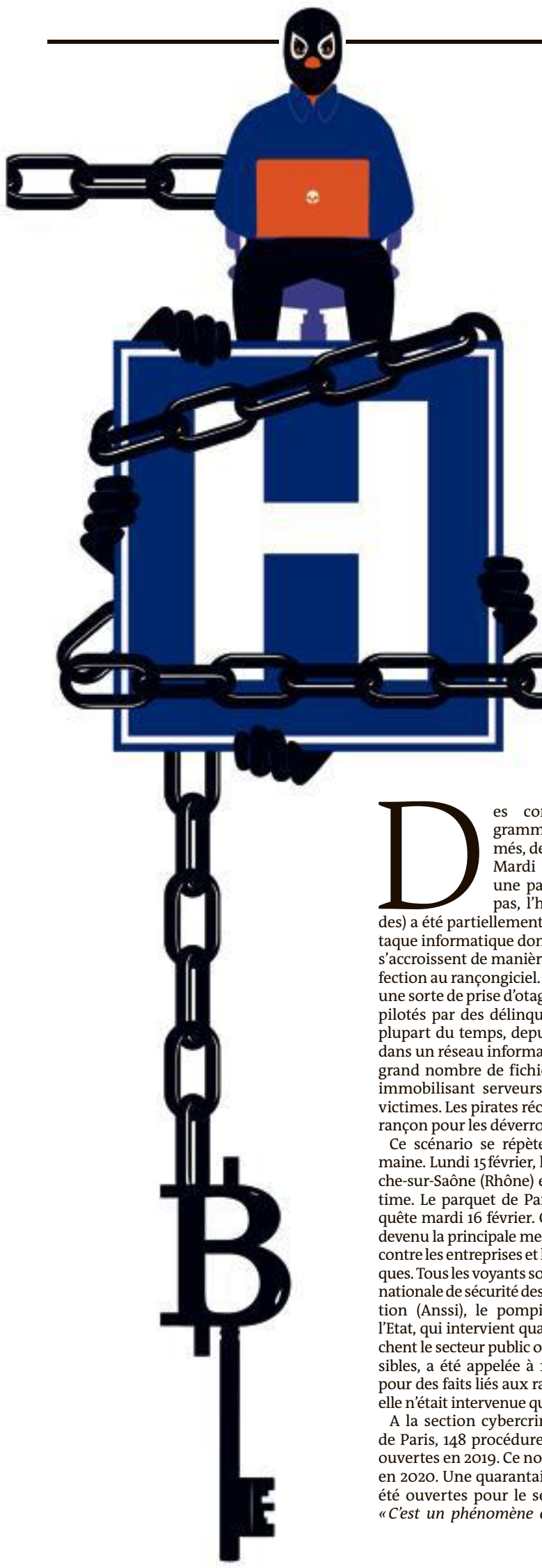
L'annuaire de codes postaux datant 1989 est ressorti pour pouvoir envoyer les courriers. « *C'est là qu'on s'aperçoit à quel point on est dépendant de l'informatique. Surtout, on a l'impression de régresser* », témoigne un agent, alors que le retour au papier allonge toutes les procédures.

Priorité pour la direction du système d'information de la ville : redémarrer la messagerie professionnelle, permettre aux agents de se connecter depuis leur smartphone ou des ordinateurs portables, et assurer le paiement des salaires. Elle est épaulée par l'Agence nationale de la sécurité des systèmes d'information (Anssi) et une société qui l'aident à reconstruire un nouveau système informatique. « *Avec le Covid, avec toutes les procédures à distance et le télétravail, nous avons continué à mettre sur nos serveurs des fonctionnalités qui autrefois n'existaient pas. Nous nous sommes beaucoup plus concentrés sur le fait d'augmenter les services offerts à la population via le numérique qu'au fait de protéger l'architecture de ces systèmes*, reconnaissait le maire d'Angers, Christophe Béchu, dans une interview au média Brut. *Ça ne veut pas dire que nous n'avons rien fait, mais que nous n'avons pas mis assez d'intensité et d'efforts là-dessus.* »

Un mois après, la situation n'est pas encore tout à fait revenue à la normale pour la mairie. Mais aucune donnée ne semble, à ce stade, avoir été exfiltrée. Le risque que des pirates puissent envoyer des mails frauduleux aux Angevins est donc a priori écarté. Ces derniers peuvent se poser une autre question : quel sera le coût pour la collectivité ? ■

**L. V.**

Le Monde
JEUDI 18 FÉVRIER 2021



PIRATAGE INFORMATIQUE

# Comment la France affronte le « cyberfléau » des rançongiciels

Les attaques contre des hôpitaux ou des entreprises sensibles ont coûté, l'an dernier, des centaines de millions d'euros. La fréquence et la gravité des raids s'intensifient

ENQUÊTE

Des consultations déprogrammées, des services fermés, des soignants affolés… Mardi 9 février, comme si une pandémie ne suffisait pas, l'hôpital de Dax (Landes) a été partiellement paralysé par une attaque informatique dont le type et la gravité s'accroissent de manière alarmante : une infection au rançongiciel. Ces virus se livrent à une sorte de prise d'otage numérique et sont pilotés par des délinquants qui opèrent, la plupart du temps, depuis l'étranger. Lâchés dans un réseau informatique, ils rendent un grand nombre de fichiers inaccessibles, en immobilisant serveurs et ordinateurs des victimes. Les pirates réclament, ensuite, une rançon pour les déverrouiller.

Ce scénario se répète semaine après semaine. Lundi 15 février, l'hôpital de Villefranche-sur-Saône (Rhône) en a été lui aussi victime. Le parquet de Paris a ouvert une enquête mardi 16 février. Ce type d'attaque est devenu la principale menace cybercriminelle contre les entreprises et les institutions publiques. Tous les voyants sont au rouge. L'Agence nationale de sécurité des systèmes d'information (Anssi), le pompier informatique de l'Etat, qui intervient quand des attaques touchent le secteur public ou les entreprises sensibles, a été appelée à 192 reprises en 2020 pour des faits liés aux rançongiciels. En 2019, elle n'était intervenue qu'à 54 reprises.

A la section cybercriminalité du parquet de Paris, 148 procédures de ce type ont été ouvertes en 2019. Ce nombre est passé à 436 en 2020. Une quarantaine d'autres ont déjà été ouvertes pour le seul mois de janvier. *« C'est un phénomène exponentiel »,* se désole Johanna Brousse, qui dirige la section. Grand ou petit, célèbre ou anonyme : aucun organisme n'est à l'abri. En France, les collectivités locales ont payé un lourd tribut ces derniers mois – la ville et la métropole d'Angers figurent parmi les victimes récentes. Ces virus n'épargnent pas non plus les hôpitaux, comme le déplore Mme Brousse : *« Ce sont des criminels sans foi ni loi. Ils se disent que, s'ils touchent un hôpital en période de Covid, l'Etat va payer. »*

**DANS LES USINES, LES MACHINES S'ARRÊTENT. LES TÉLÉPHONES DEVIENNENT MUETS. LES LOGICIELS DE PAYE NE RÉPONDENT PLUS**

S'en prenant à l'informatique, système nerveux central des entreprises, une attaque au rançongiciel peut être dévastatrice. Dans les usines, les machines s'arrêtent. Les boîtes courriels sont inutilisables, les téléphones deviennent muets. Les logiciels de comptabilité ou de paye ne répondent plus. Après la déflagration, il faut parfois plusieurs mois aux victimes pour retrouver un fonctionnement correct – sans parler de l'argent perdu.

Ainsi, l'attaque contre l'entreprise de services et conseil Sopra Steria, l'année dernière, a coûté entre 40 et 50 millions d'euros. Le groupe de laboratoires d'analyses Eurofins Scientific, touché en 2019, a, lui, perdu 69 millions d'euros sur son chiffre d'affaires. L'entreprise de conseil Altran et le poids lourd norvégien de l'aluminium Norsk Hydro ont respectivement perdu 20 millions d'euros et plus de 49 à 58 millions d'euros avant le remboursement des assurances. *« Les grands groupes ont une assise suffisamment solide pour s'en remettre, mais un rançongiciel peut faire mettre la clé sous la porte à une PME ou à une TPE »,* craint François Deruty, sous-directeur des opérations de l'Anssi. Les rançongiciels ne sont pas nouveaux. Mais plusieurs facteurs les ont rendus, ces deux dernières années, plus visibles et destructeurs. Les pirates, de plus en plus riches, professionnels et organisés, mènent maintenant des attaques ciblées et retentissantes. *« En 2020, nous avons vu apparaître des familles* [de rançongiciels] *beaucoup plus agressives. On sent qu'il y a derrière une équipe plus structurée, ciblant des sociétés beaucoup plus puissantes, avec des rançons qui vont jusqu'à plusieurs millions d'euros »,* décrypte la colonelle Fabienne Lopez, qui dirige le C3N, l'unité spécialisée de la gendarmerie.

**PUBLICATION DES DOCUMENTS VOLÉS**

Les cybercriminels ont aussi développé de nombreuses stratégies pour se faire payer la rançon. Fin 2019, le groupe derrière le rançongiciel Maze a innové : pour faire plier une victime réticente à payer, il menace de publier une partie des documents volés. Cette technique a depuis été adoptée par la quasi-totalité des groupes cybercriminels. Désormais, plus de vingt groupes disposent de portails en ligne sur lesquels ils publient – ou affirment publier – les secrets d'entreprises récalcitrantes.

Des centaines de victimes, y compris françaises, en ont déjà fait les frais. Et, lorsque l'entreprise refuse toujours de payer une rançon pour débloquer la situation, certains poussent le vice jusqu'à proposer un système d'enchères, ouvert à tous, pour monétiser les documents volés.

Si les attaques par rançongiciels déferlent ainsi, c'est aussi parce qu'elles rapportent gros. Les rançons demandées par les cybercriminels ont fortement augmenté et atteignent régulièrement la dizaine de millions d'euros. Et les entreprises paient, même lorsque cela leur est fortement déconseillé par les autorités. La plupart des experts estiment qu'une victime sur cinq règle la rançon. Selon Chainalysis, une entreprise spécialisée dans l'analyse des cryptomonnaies,

## Derrière les virus, un cercle très fermé de criminels venus de l'Est

Les acteurs importants du rançongiciel sont souvent d'origine russe, ou russophones, et échappent généralement aux autorités

De l'extérieur, le petit pavillon beige de Gatineau, au Québec, est loin de l'idée que l'on se fait du repaire d'un pirate informatique. Pourtant, son occupant, Sébastien Vachon-Desjardins, y a été arrêté : il aurait extorqué plus de 22 millions d'euros à l'aide d'un rançongiciel, un programme informatique malveillant qui rend les données de ses victimes inaccessibles et exige un paiement pour les déverrouiller. La justice américaine l'accuse en particulier d'avoir inséré le rançongiciel Netwalker, l'un des plus virulents, dans les réseaux informatiques de nombreuses entités.

**De très rares interpellations**

Ce type d'interpellation est rarissime. Habituellement, les pirates interpellés pour des faits de rançongiciels sont le plus souvent des petites mains de la cybercriminalité, des complices, qui aident à ce que des infections aient lieu. En août, un Russe a par exemple été arrêté pour avoir tenté de convaincre un employé de l'usine Tesla de Reno (Nevada) d'insérer un rançongiciel dans le réseau de l'entreprise, en échange d'une récompense d'un demi-million de dollars. Mais les actuels gros bonnets du rançongiciel ont échappé jusqu'ici aux autorités, protégés par leur habileté technique, avec des paiements en cryptomonnaies – difficiles à tracer – et des serveurs informatiques hébergés par des entreprises imperméables aux réquisitions judiciaires. Loin de l'image du pirate ingénieux et créatif opérant depuis sa chambre d'adolescent, il est ici question de délinquants aguerris, mus – sauf exceptions – par le seul appât du gain, sans scrupule et parfaitement organisés.

Certains groupes sont liés par des relations de longue date avec d'autres pirates, dont ils ne connaissent parfois que les pseudonymes sur les forums ou les messageries instantanées sécurisées. Où sont-ils basés ? Les preuves sont limitées, mais elles pointent très souvent dans la même direction. *« En nous basant sur leur code informatique, leur langue, les heures auxquelles ils sont actifs, on peut dire qu'il y a une prédominance d'individus russes ou russophones derrière de nombreux rançongiciels. Mais ils ne sont bien sûr pas les seuls »,* explique John Shier, expert de la société de sécurité informatique américaine Sophos.

Beaucoup de rançongiciels sont conçus pour ne pas s'activer sur les ordinateurs configurés dans certaines langues, comme le russe, le kazakh, le syrien ou l'ukrainien. *« Souvent, ceux qui plongent dans le cybercrime ont été des adolescents très doués, à l'aise avec les ordinateurs »,* décrypte Robert McArdle, expert en cybercrime pour l'entreprise TrendMicro. *« En Russie, il y a un des meilleurs systèmes éducatifs du monde en matière d'informatique et de mathématiques, mais les perspectives d'emploi ne sont pas aussi bonnes qu'en Occident. Cela mène naturellement certains vers le cybercrime »,* poursuit-il. *« Ce sont des gens qui font ça depuis dix ans. S'ils ont commencé lorsqu'ils avaient la vingtaine, ils ont aujourd'hui au moins 30, voire 40 ans. Cela signifie qu'ils ont une famille, des enfants à aller chercher à l'école »,* précise Robert McArdle.

**Un écosystème très dense**

Combien y a-t-il de cybercriminels impliqués dans le rançongiciel ? Impossible de le dire. Certains groupes développant et vendant des logiciels malveillants affirment être forts d'une dizaine de développeurs.

Selon plusieurs experts interrogés, le rançongiciel est devenu tellement lucratif qu'il a attiré des pirates venus d'autres secteurs de la cybercriminalité. Mais cette branche recouvre un nombre restreint de cybercriminels. *« Cela reste un milieu fermé, ce sont des vieux acteurs qui se connaissent depuis longtemps* (…). *Ce sont les mêmes personnes qui sont là depuis dix ans »,* précise Benoît Ancel, expert d'une entreprise spécialisée en cybercriminalité. Evil Corp, par exemple, est un groupe cybercriminel apparu il y a sept ans sur les ruines du Business Club, un autre gang. A sa tête se trouve, selon la justice américaine, Maksim Yakubets, un Russe de 34 ans. Evil Corp est à l'origine des logiciels malveillants les plus néfastes de ces dix dernières années, notamment le « malware » bancaire Dridex. L'industrie de la cybersécurité considère aujourd'hui Evil Corp et ses émanations à l'origine de rançongiciels plus récents : Doppelpaymer, BitPaymer et WastedLocker. Les liens qui les unissent à TA505, autre groupe désormais spécialisé dans les rançongiciels, sont très étroits. Evil Corp est par exemple aussi lié avec le groupe développant le logiciel malveillant Trickbot. Une partie des gangs sont contraints à une forme de publicité. La réputation des uns et des autres, dans ce milieu, est fragile et précieuse.

**« EN RUSSIE, IL Y A UN DES MEILLEURS SYSTÈMES ÉDUCATIFS DU MONDE EN MATIÈRE D'INFORMATIQUE ET DE MATHÉMATIQUES »**

ROBERT MCARDLE
expert en cybercrime

Un certain nombre de pirates présentent par ailleurs leur activité comme un service rendu à des *« clients »* ou des *« partenaires »*. Comprendre : leurs victimes. Certains prétendent suivre un code de conduite et ne pas viser des hôpitaux en période de pandémie. Une parole qui n'engage qu'eux : de nombreuses attaques par rançongiciel ont eu lieu pendant la pandémie, et en particulier, ces derniers jours en France, à Dax ou à Villefranche-sur-Saône. ■

A. DE., F. RE. ET M. U.


# Le traumatisme des salariés victimes des « gangs » du Net

Les réseaux informatiques et les ordinateurs des entreprises piratées peuvent être totalement paralysés. Parfois choqués, les salariés touchés se retrouvent souvent au chômage technique

*Il y avait un écran tout bleu m'informant que mes dossiers avaient été cryptés, et qui me demandait à peu près 2 000 euros. J'avais envie de pleurer.* » En 2016, Julie Wernert, chef d'entreprise dans les Bouches-du-Rhône, a vécu un scénario qu'ont vécu depuis des milliers de professionnels en France. Après avoir cliqué sur une pièce jointe infectée par un logiciel malveillant, son ordinateur, qui lui sert à la fois de poste de travail professionnel et personnel, a été la cible d'un rançongiciel : un virus qui chiffre les fichiers d'une machine et demande le paiement d'une rançon pour les récupérer.

« *On a remonté une sauvegarde, mais elle datait de fin 2015, donc j'avais à peu près huit mois de travail à refaire* », se rappelle-t-elle. Devis, factures, documents fiscaux… Au total, 4 652 documents ont été chiffrés par le rançongiciel. Par chance, des copies sur papier avaient été conservées, mais il a fallu « *grosso modo* » un mois pour tout saisir de nouveau informatiquement. « *Il y a eu du retard de pris sur les chantiers parce qu'on n'avait plus nos devis* », explique cette chef d'une TPE du bâtiment.

**« ON A EU DES CAS D'ENTREPRISES QUI SE SONT MISES AU CHÔMAGE TECHNIQUE PENDANT UNE BONNE SEMAINE »**

**DAVID CAILLAT**
manager chez Amossys

### « Sidération totale »

2016 était une autre époque, une éternité pour une cybercriminalité qui évolue à toute vitesse. Les opérateurs de rançongiciels tapaient plus large, visant aussi bien les petites sociétés que les particuliers. En 2021, la majorité des attaques restent opportunistes (elles visent des réseaux peu sécurisés), et les groupes qui les mènent sont mieux organisés, et font plus de dégâts, laissant généralement les particuliers tranquilles et se concentrant sur les multinationales et les collectivités locales. Les réactions des victimes, lorsqu'elles prennent conscience de l'attaque, sont presque universelles cependant.

« *On se sent un peu démuni, abandonné parce qu'il n'y a pas un médecin qui vient vous soulager, comme quand vous êtes malade* », abonde une avocate dont le cabinet a été touché par un rançongiciel il y a environ cinq ans, et qui souhaite garder l'anonymat. Comme Julie Wernert, son premier sentiment fut la panique : « *On devient très vite parano, on se demande si nos données sont accessibles à d'autres.* »

« *Il y a une phase de sidération totale,* [les entreprises] *ne comprennent pas ce qui leur arrive* », raconte Pauline Donon, responsable de la gestion de crise pour Intrinsec, une entreprise de réponse à incident. « *Souvent, on arrive dans l'heure ou les deux premières heures après le début de la crise.* (…) *Il y a des gens qui courent un peu partout dans les couloirs. Il y a des gens aussi qui sont complètement désœuvrés* », relate Gérôme Billois, expert pour l'entreprise Wavestone. Kilian Lavieille, responsable du centre d'alerte et de réaction aux attaques informatiques (CERT, en anglais) chez Intrinsec, se souvient d'une intervention sur un cas critique dans une entreprise : « *On a eu le RSSI* [responsable de la sécurité des systèmes d'information] *en pleurs, qui ne savait pas quoi faire. Au début, on fait comme les pompiers et on donne une liste de tâches à faire.* »

**« ON SE SENT UN PEU DÉMUNI, IL N'Y A PAS UN MÉDECIN QUI VIENT VOUS SOULAGER COMME QUAND VOUS ÊTES MALADE »**

**UNE AVOCATE**

Plus la taille de l'entité ciblée est grande, plus les dégâts peuvent être importants, dès lors que des milliers d'ordinateurs connectés en réseau peuvent être paralysés. C'est ce qui s'est passé à Marseille, en mars 2020, lorsque la ville et la métropole Aix-Marseille-Provence ont été touchées par un rançongiciel. « *Le pire cauchemar* (…), *une compromission généralisée, un* ransomware [rançongiciel] *une veille d'élection et une veille de confinement : les conditions idéales pour une crise parfaite* », s'est souvenu Jérôme Poggi, responsable de la sécurité des systèmes d'information de la mairie, lors d'une intervention à la conférence sur la cybercriminalité Panocrim**,** début janvier.

Malgré cette panique générale, les interlocuteurs s'accordent pour affirmer que ces attaques n'entraînent pas de représailles contre les salariés dont le poste de travail a pu servir de point de départ à l'infection. « *On reçoit beaucoup d'e-mails de gens à l'international avec parfois juste une photo. C'est un mail sur lequel je pourrais recliquer* », reconnaît Julien, salarié d'une entreprise parisienne qui a ouvert une pièce jointe infectée il y a quelques années, entraînant la paralysie du réseau. « *Le pauvre garçon, il n'y est pour rien, c'était un mail assez bien foutu* », défend une de ses collègues, Catherine (les prénoms ont été modifiés à la demande des personnes).

« *On n'a jamais vu de cas où des salariés étaient pris à partie ou subissaient des pressions. On a en revanche vu des salariés un peu paniqués qui avaient peur d'avoir mal fait quelque chose* », abonde Alexandre Deloup, responsable du CERT pour la société Amossys.

### « Il faut qu'on redémarre »

Très vite, après une attaque, un plan de secours doit être mis en place pour assurer la communication entre les salariés et la direction et pour minimiser la perte d'activité. Il faut être capable de travailler sans e-mail, parfois sans téléphone fixe. Un ancien cadre municipal d'une grande agglomération française touchée récemment se souvient : « *On a fait des groupes WhatsApp pour tout et on a mis en place une messagerie de secours, un système de visioconférence, etc.* »

Combien de temps faut-il pour se rétablir d'une telle attaque ? Là encore, les données sont très variables d'une situation à l'autre. Une très petite entreprise qui avait mis à l'abri des sauvegardes récentes de son système informatique peut très bien rétablir l'activité en une journée ou moins. Si l'incident est majeur et paralyse toute l'infrastructure dans une grande société, « *reprendre une activité partielle ne se fait pas avant deux semaines* », juge, chez Intrinsec, Kilian Lavieille. « *On a eu des cas d'entreprises importantes qui se sont mises au chômage technique pendant une bonne semaine* », ajoute David Caillat, manager chez Amossys. « *Il faut trois à six mois pour revenir vraiment à la normale* », précise de son côté Pauline Donon, d'Intrinsec, qui explique que « *toutes les activités critiques* [de l'entreprise] *vont être priorisées, et* [que] *certaines activités un peu moins critiques vont être oubliées, comme des services administratifs annexes* ».

Pendant les premiers jours, parfois très difficiles, Pauline Donon explique être souvent « *prise entre deux feux* » car « *les responsables business vont clairement vouloir redémarrer le plus tôt possible et dire : "On perd de l'argent, il faut qu'on redémarre."* » De leur côté, les enquêteurs et les prestataires doivent pouvoir enquêter, mais surtout guider les responsables du service informatique pour reconstruire une infrastructure et empêcher de subir une nouvelle attaque. Tous les enquêteurs interrogés par *Le Monde* s'accordent à dire que trop de victimes continuent de ne pas porter plainte lorsqu'elles sont touchées. A l'heure actuelle, avec une seule affaire liée à un rançongiciel jugée devant un tribunal français, les victimes peuvent se sentir découragées. Les enquêtes, très techniques et toujours internationales, se heurtent à la fois aux méthodes de dissimulation des criminels et à la difficulté de faire coopérer certains pays, ce qui prend beaucoup de temps.

### « L'espoir d'une justice »

« *Comme beaucoup de Français, on* [porte plainte] *pour l'assurance, pour la forme, et dans l'espoir d'une justice*, lâche, un peu résigné, le maire d'une petite commune française. *Qu'est-ce que vous voulez ?* [Les coupables] *ne sont probablement même pas en France.* » En 2020, sa commune a été frappée par un rançongiciel, et les auteurs ont récemment mis en ligne plusieurs gigaoctets de données dérobées à la mairie.

Lorsque, quatre ans plus, tôt Julie Wernert a porté plainte, elle n'avait pas grand espoir non plus : « *Je suis partie du principe que s'il y avait une chance sur un million il fallait la saisir.* » Quelques mois plus tard, elle a reçu un courrier lui faisant savoir que l'affaire allait être classée faute d'éléments nouveaux. Alors quand, en 2019, elle a de nouveau été frappée par un rançongiciel, elle n'a pas porté plainte. « *Vu que j'avais fait mes sauvegardes correctement, j'ai tout récupéré en moins de dix minutes ; j'aurais perdu plus de temps* [à déposer plainte] *qu'à récupérer les données* », explique-t-elle.

Pourtant – elle l'ignorait à l'époque –, quelques mois plus tard, sa première plainte aboutit, et elle est invitée par le tribunal de Paris à se constituer partie civile dans le procès d'Alexander Vinnik. Le Russe, alors soupçonné d'avoir opéré le rançongiciel Locky, a finalement été condamné pour blanchiment d'argent en décembre 2020. « *Aujourd'hui, si ça m'arrivait de nouveau, j'irais porter plainte* », assure la chef d'entreprise. ■

F. RE. ET M. U.

les gangs de rançongiciels ont empoché au moins 350 millions de dollars (environ 288 millions d'euros) en 2020. C'est 311 % de plus qu'en 2019. Une estimation pourtant très prudente : l'Agence de cybersécurité européenne compte que 10 milliards d'euros en rançon ont été payés en 2019.

Les hackeurs peuplant l'écosystème du rançongiciel « *peuvent quasiment agir en toute impunité* ». Les mots, sévères, sont ceux de l'agence Europol. En France, un seul suspect dans une affaire a été jugé, en octobre 2020. Condamné pour blanchiment, il a été relaxé des faits liés au rançongiciel et a fait appel. Un deuxième procès en France dans une affaire de rançongiciel ayant visé une banque anglaise va se tenir. Mais les interpellations pour des faits liés aux rançongiciels demeurent très rares.

### FLUX DE CRYPTOMONNAIES

« *C'est extrêmement compliqué de trouver les auteurs* », convient Catherine Chambon, à la sous-direction de la lutte contre la cybercriminalité. Cette impunité s'explique aussi par les moyens judiciaires déployés jusqu'ici. En France, pour enquêter sur près de six cents attaques, le parquet ne comporte que trois magistrats spécialisés, et quelques dizaines d'enquêteurs en police et en gendarmerie se consacrent spécialement à la cybercriminalité.

Du reste, beaucoup d'observateurs considèrent que les rançonneurs sont protégés. Ces derniers parlent souvent russe, codent sur les fuseaux horaires de Russie et d'Europe de l'Est et conçoivent leurs logiciels pour qu'ils épargnent cette zone géographique. « *Les attaques sont menées depuis des pays où, parfois, les autorités protègent ces cybercriminels. Il faudra que ça change, y compris dans l'intérêt de ces autorités* », a averti Guillaume Poupard, le directeur de l'Anssi lors d'une récente conférence. Les rançongiciels « *sont utilisés par des Etats pour le sale boulot… du moment qu'ils ne s'attaquent pas à l'Etat dans lequel ils se trouvent* », affirme Mme Chambon. Certains Etats « *peuvent désigner* » des cibles, dénonce même la haut gradée. Cette protection serait, pourtant, « *minoritaire* », selon Johanna Brousse, du parquet de Paris, qui s'est rendue en décembre en Russie pour des perquisitions et des auditions. « *On collabore bien avec les Russes, contrairement à ce qu'on pourrait penser* », nous explique la magistrate. Face à l'ampleur du phénomène, les autorités se sont organisées et promettent des résultats. Depuis 2018, une partie des agents de l'Anssi pistent et analysent les différents acteurs de l'écosystème du rançongiciel. « *Le rançongiciel est la principale priorité des prochaines années* », explique Edvardas Sileris, le chef de l'unité cyber d'Europol.

La moitié des quatre cents enquêtes coordonnées au sein de sa structure concernent aujourd'hui des rançongiciels. En matière judiciaire, en France, 2020 a été un « *tournant* », veut croire Johanna Brousse. Depuis février 2020, les travaux des trois services français d'enquête spécialisés en cybercriminalité sont mieux articulés. Une base de données rassemblant les éléments techniques de toutes les enquêtes a été mise en place afin de faciliter les recoupements. Les experts de l'Etat en la matière se réunissent quasiment toutes les semaines pour échanger sur les dernières évolutions du domaine.

De « *grosses avancées* », selon les termes de Fabienne Lopez, ont, enfin, été réalisées récemment dans le suivi des flux de cryptomonnaies. Tracfin est aussi entré dans la danse. Au sein du service de renseignement financier, une cellule d'enquête « cyber » a été créée en 2018, et des enquêteurs spécialisés dans la blockchain ont été recrutés. Dans plusieurs dossiers, les enquêteurs sont parvenus à identifier nommément des individus malgré leur utilisation de mixeurs, des services censés brouiller les flux de bitcoins. Les enquêteurs s'intéressent, par ailleurs, de très près à ces acteurs, fréquemment complices des gangs de rançongiciels.

### « CHERCHER À LES BLOQUER »

Les enquêteurs espèrent, désormais, obtenir des résultats et des interpellations. Policiers et gendarmes participent à plusieurs équipes d'enquête avec leurs homologues de divers pays européens. Certaines demandes d'entraide pénale émises par la France ont récemment abouti. Des individus soupçonnés d'avoir réalisé des attaques ont été identifiés. Une personne, aux Etats-Unis, doit être entendue et poursuivie en France prochainement. Des enquêteurs français doivent se rendre dans un pays européen pour entendre une personne suspectée d'être l'autrice d'une attaque par le biais de deux souches de *ransomwares* différents. Plusieurs mandats d'arrêt ont été émis pour des faits liés à des rançongiciels. Selon nos informations, confirmant celles de France Inter, les autorités françaises et ukrainiennes ont tout récemment mené une opération visant un rançongiciel et s'apprêtent à en annoncer les résultats. ■

ANTOINE DELAUNAY,
FLORIAN REYNAUD
ET MARTIN UNTERSINGER

Libération **Vendredi** *19 Février 2021*

# «Rançongiciels» A l'hôpital, la contagion des cyberattaques

**Déjà sept cas depuis le 1er janvier: de plus en plus de structures hospitalières, aux réseaux informatiques souvent vulnérables, sont devenues des cibles.**

Par
**ALEXANDRE HORN**

Ordinateurs déconnectés, consultations et vaccinations suspendues, stylos et papier ressortis des tiroirs: la même scène étrange se répète, depuis quelques semaines, dans plusieurs hôpitaux en France. En cause, un virus, non pas biologique mais informatique, inoculé dans les réseaux par des hackeurs malveillants.

La dernière cyberattaque en date a touché le groupe hospitalier du nord-ouest lyonnais (Villefranche-sur-Saône, Tarare et Trévoux), lundi à 4h 30 du matin. Un rançongiciel a chiffré les données de ces établissements, exigeant une somme d'argent pour les débloquer. De quoi les rendre inutilisables et entraver une partie du fonctionnement des services. *«On s'est aperçus très rapidement qu'un chiffrement était en cours, donc on a tout déconnecté pour éviter de maintenir le lien avec les attaquants,* explique Nasser Amani, directeur des systèmes numériques du groupement hospitalier. *C'est difficile de dire à quel point les données sont affectées, on termine l'état des lieux. Mais les postes de travail d'au moins trois hôpitaux sont touchés.»*

Privés d'Internet, ces centres hospitaliers fonctionnent en mode dégradé. Les chirurgies non urgentes sont reportées jusqu'à nouvel ordre et le Samu comme les pompiers réorientent leurs malades vers d'autres établissements. *«L'hôpital était déjà très sollicité avant l'attaque. On a réussi à éviter la paralysie et on assure la continuité des soins en accueillant notamment les patients qui se présentent par leurs propres moyens aux urgences. On a 576 patients hospitalisés, un service de réanimation qui tourne, mais, avec le papier plutôt que l'informatique, le temps de prise en charge est beaucoup plus long»,* poursuit Nasser Amani.

Cette cyberattaque est la septième depuis le début de l'année contre des établissements de santé en France. Et rien n'indique qu'elles vont diminuer. Depuis fin 2017, la déclaration des incidents de sécurité des établissements sanitaires est obligatoire, ce qui permet à la Direction générale de la santé (DGS) de recenser leur évolution. Or l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui accompagne la protection de ces organismes vitaux, recense, ces derniers temps, près d'une tentative par semaine.

> «Ceux qui font ça scannent des plages d'adresses IP en passant de postes en postes. Ils ne savent souvent pas vraiment qu'ils attaquent [des hôpitaux].»
>
> **Baptiste Robert**
> chercheur en cybersécurité

En 2018, première année de recensement, une trentaine d'incidents causés par des rançongiciels sur des structures sanitaires ont été déclarés. Puis 46 en 2019, et 49 en 2020. Et déjà 5 incidents déclarés en janvier 2021, auxquels on peut donc ajouter ceux de Villefranche et de Dax ce mois-ci.

L'hôpital de Dax, dans les Landes, a en effet été visé, le 9 février, par une cyberattaque. Un rançongiciel a infecté les systèmes informatiques avec un mode opératoire proche, chiffré les données pour les rendre inaccessibles aux personnels, puis demandé une rançon. *«Le système informatique s'est dégradé petit à petit, jusqu'à ne plus fonctionner du tout,* témoigne le maire de Dax, Julien Dubois. *Il n'était plus possible de recevoir en cancérologie et en radiologie, car cela nécessite d'avoir le dossier du patient, qui est informatisé. La vaccination s'est arrêtée également, mais a pu reprendre rapidement. On a eu un problème sur la gestion de la logistique qui se faisait, elle aussi, par informatique.»* L'hôpital, depuis, continue de tourner, mais difficilement. *«On est toujours avec des procédures dégradées, et ça va durer au moins deux semaines.»*

### «LA RÈGLE EST CLAIRE, ON NE NÉGOCIE PAS»

Cette intensification des cyberattaques n'est pas propre au secteur de la santé, comme l'explique Ivan Fontarensky, responsable technique cyberdéfense chez Thales, une des entreprises appelées à répondre à ce genre d'agressions: *«Ces dernières années, la cybercriminalité a explosé. Entre octobre 2019 et octobre 2020, on a connu une multiplication par 20 des cyberattaques.»* Parmi elles, le rançongiciel s'est imposé comme la principale des menaces. Facile d'utilisation, demandant peu de compétences techniques, il s'est révélé très efficace. *«Il existe à la marge des attaques d'activistes, de cyberterroristes ou sponsorisées par des Etats. Mais pour les cybercriminels comme ici, l'objectif est simple: récupérer de l'argent. Et avec ces logiciels de rançon, ça marche. Les victimes payent pour retrouver leurs données ou pour qu'elles ne soient pas dévoilées, et cette efficacité a aidé à l'explosion de ce phénomène.»*

Les hôpitaux, eux, ne payeraient pas les rançons, perdant du même coup l'accès à leurs données et à leurs systèmes informatiques. *«La règle est claire, on ne négocie pas avec les attaquants»,* déclare la DGS. Ce que confirme Nicolas Arpagian, vice-président en charge de la stratégie chez Orange Cyberdefense, la branche cybersécurité de l'opérateur: *«En France, jamais un hôpital n'a payé ce genre de rançon. Ce n'est pas illégal, mais de facto, un organisme public financerait alors une organisation criminelle.»*

Même avec l'intervention de professionnels de la cybersécurité, le retour à la normale reste cependant difficile pour les Suite page 4


Emmanuel Macron en visioconférence avec les responsables des


**hôpitaux de Dax et de Villefranche-sur-Saône, jeudi, depuis l'Elysée.** PHOTO MARC CHAUMEIL

ÉDITORIAL

Par
**DOV ALFON**

## Blinder les ambulances

On ne tire pas sur une ambulance, dit le dicton populaire, et pourtant c'est exactement ce qui s'est passé lundi dans la nuit à l'hôpital de Villefranche-sur-Saône : un attaquant informatique a bloqué les données de tout le groupe hospitalier du nord-ouest lyonnais, exigeant une rançon pour les débloquer. Le centre hospitalier fonctionne depuis en mode dégradé et le Samu doit réorienter ses malades vers d'autres établissements. C'est la septième attaque de ce genre depuis le début de 2021. La campagne de vaccination des personnes à risque a dû être retardée à l'hôpital de Dax, dans les Landes, visé le 9 février par une action similaire. Au milieu d'une pandémie meurtrière, les conséquences potentielles de ces attaques sont terrifiantes. La cybersécurité n'a jamais été aussi vitale pour les hôpitaux qu'elle ne l'est actuellement. Or en France comme dans beaucoup d'autres nations riches et informatisées, les hôpitaux sont très mal protégés contre ce genre d'attaques, quelquefois mortelles. La première victime documentée date de septembre 2020 : une patiente arrivée dans un état critique à l'hôpital de Düsseldorf en Allemagne juste quand un attaquant avait paralysé les équipements informatiques du service des urgences est morte lors de son transfert vers un hôpital plus éloigné. Le président de la République a annoncé jeudi une accélération de la stratégie nationale en matière de cybersécurité, un plan à 1 milliard d'euros (dont 720 millions de financements publics) sur plusieurs années. D'ici là, il est important de tenir bon en refusant de payer la moindre rançon, un acte immoral qui ne manquerait pas d'attirer vers les hôpitaux français tous les criminels informatiques de la planète. Comme l'a justement pointé Emmanuel Macron, il en va aussi de la responsabilité individuelle du personnel hospitalier, qui doit accroître sa vigilance en matière de mots de passe et logiciels à distance. Car on tire sur des ambulances, mieux vaut donc les blinder.

# Un milliard d'euros pour la contre-attaque

**Pour faire face à la menace croissante des attaques informatiques, Emmanuel Macron a annoncé jeudi vouloir investir largement dans la recherche-développement, le renforcement de la formation et la sensibilisation du grand public.**

Quand on le cyberattaque, l'Etat contre-attaque. Emmanuel Macron a détaillé jeudi les grandes orientations de l'accélération de la stratégie nationale en matière de cybersécurité, alors que les offensives numériques se multiplient ces derniers mois sur le territoire. D'après l'Agence nationale de la sécurité des systèmes d'information (Anssi), elles auraient été multipliées par quatre entre 2019 et 2020, passant ainsi d'une cinquantaine à 200 en ce qui concerne les «opérateurs d'importance vitale».
Ces derniers temps, ce sont les hôpitaux qui sont les cibles privilégiées des hackers. En quelques jours seulement, les établissements de Dax (Landes) et de Villefranche-sur-Saône (Rhône) ont été victimes de «rançongiciels», une attaque qui consiste à bloquer les données d'un système informatique et de ne les rendre accessibles qu'après paiement d'une rançon *(lire pages 2-4)*.

**«En quelques instants».** Le chef de l'Etat s'entretenait justement avec les responsables des centres hospitaliers en question jeudi, en visioconférence. *«Vos retours montrent bien que ces attaques cyber, qui peuvent paraître très abstraites, qui ne faisaient pas partie du quotidien de notre pays et dont on parlait peu, peuvent en quelques instants venir percuter tout un système d'organisation»*, leur a-t-il déclaré, insistant notamment sur le fait qu'il s'agit d'*«une menace extrêmement sérieuse, parfois vitale, qui touche tous les secteurs»*.
Pour faire face à cette *«menace»*, le gouvernement a présenté un plan à 1 milliard d'euros (dont 720 millions de financements publics) et fixé plusieurs grands objectifs à l'horizon 2025. Tout d'abord, l'Etat veut investir massivement pour encourager la recherche et le développement de nouvelles technologies afin de créer un *«écosystème»* mieux armé pour repérer les attaques plus vite et y remédier de façon plus efficace. 500 millions d'euros y seront consacrés.
Dans cette optique, un cybercampus ouvrira ses portes en septembre. Un complexe qui regroupera entreprises, institutions et laboratoires spécialisés dans le domaine afin de coordonner les moyens pour lutter au mieux contre les attaques. D'ici à 2025, le gouvernement souhaite aussi doubler le nombre d'emplois dans le secteur et multiplier par trois le chiffre d'affaires de la filière. *«L'objectif de ce plan est de renforcer les formations dans le domaine de la cybersécurité»*, a également avancé Emmanuel Macron. Ainsi, dans le secteur de la santé notamment, les établissements seront invités à consacrer systématiquement entre 5 % et 10 % de leurs budgets numériques à la cybersécurité et à la formation de leurs personnels.

**«Le Bureau des légendes».** Enfin, le chef de l'Etat veut mettre l'accent sur la sensibilisation. *«Le sujet de l'acculturation est essentiel*, estime-t-il. *Pas besoin d'être expert pour déjouer la plupart des cyberattaques. Elles s'appuient souvent sur des négligences, sur un mot de passe trop évident, un oubli de mise à jour, une demande suspecte par mail.»*
Sur son compte Twitter, l'Elysée a déjà lancé sa campagne de sensibilisation en publiant une courte vidéo directement inspirée de la série *le Bureau des légendes* invitant les internautes à *«adopter les bons réflexes pour déjouer les attaques»*.

**SACHA NELKEN**

# «On ouvrait des mails sans savoir qui était l'expéditeur...»

**Mairies, intercommunalités... Les collectivités locales subissent elles aussi l'assaut des pirates informatiques, qui dégradent le service public. Et cherchent la parade.**

KANAWAT THONGROD . EYEEM . GETTY IMAGES

Ils se sont invités pour Noël. Leur nom: *«Netwalker». «Ce sont des gens très pointus qui sont rentrés secrètement dans nos systèmes vers le milieu du mois de décembre»*, se souvient amer Jean-François Fountaine, le maire (divers gauche) de La Rochelle. Comme Alfortville, Cognac, Marseille, ou encore cette semaine Angers, la préfecture de Charente-Maritime fait partie de ces collectivités victimes de cyberattaques. Soit l'assaut de pirates informatiques qui ont rendu momentanément inutilisables leurs matériels et exigé une rançon. Naguère totalement ignorés des collectivités locales, les enjeux liés à la cybersécurité sont de plus en plus présents à l'esprit des élus locaux. Une prise de conscience qui progresse à mesure que les piratages se multiplient.

*«Pour répondre, on a fait appel à des prestataires extérieurs mais la plus grosse dépense, c'est le temps pris par nos personnels*, explique Fountaine. *Pendant trois semaines, le service public a été altéré à La Rochelle.»* Dans l'épreuve, les services municipaux ont bénéficié des conseils de la gendarmerie et de la méthodologie de l'Agence nationale de la sécurité des systèmes d'information (Anssi) qui les a guidés pour nettoyer, secteur par secteur, leurs ordinateurs. *«Pour être honnête, on ne s'attendait pas à ça*, reconnaît le maire. *Il y avait des pare-feu mais, à l'évidence, ce n'était pas suffisant. On est plus sensibles qu'avant à ce sujet et nous allons envoyer nos cadres informatiques en formation.»*

**Pièces jointes et mots de passe.** Anne Le Henanff, première adjointe de Vannes (Morbihan), a pris conscience de ce nouveau type de menace en 2016. Plusieurs villes de l'Ouest sont alors attaquées par des pirates qui demandent une rançon. *«A l'époque, on n'était pas sensibilisés plus que ça, les agents pouvaient ouvrir des mails sans trop savoir qui était l'expéditeur»*, raconte-t-elle. A partir de là, la mairie décide de monter en compétence. Anne Le Henanff commence à travailler avec quelques experts sous la direction de l'Anssi, à la rédaction d'un guide pour sensibiliser les maires à la cybersécurité. Il paraît en novembre, en collaboration avec l'Association des maires de France (AMF). *«Beaucoup d'acteurs se sont emparés du sujet et notamment les organisations étatiques, comme l'Anssi*, se félicite-t-elle. *Mais, sur le terrain, les élus n'ont pas le temps de lire tous les guides: d'où l'importance qu'il y ait des relais, comme les associations d'élus, qui fournissent de l'information.»* Anne Le Henanff ne manque pas un colloque ou un séminaire pour sensibiliser ses pairs sur ces sujets. Pour elle, la cybersécurité est d'abord une question de bonnes pratiques et de rigueur.

*«C'est un peu comme pour le Covid, la première réponse, ce sont les bons gestes»*, abonde Claude Riboulet, président du conseil départemental de l'Allier et «monsieur numérique» pour l'Assemblée des départements de France. Ne pas ouvrir de pièce jointe quand on ne connaît pas l'expéditeur ou changer son mot de passe tous les mois, par exemple, réduit fortement le risque d'attaques. Mais de plus en plus de prestataires publics ou privés proposent aux collectivités de leur faire des audits. Ainsi, Jean-Pierre Mordant, adjoint dans une commune de 3000 habitants, en Charente-Maritime, a mené une étude complète de son système informatique. Coût total: 12000 euros.

**«Coût exorbitant».** Un effort financier qui fait reculer de nombreuses collectivités. *«C'est au niveau des intercommunalités que ces investissements doivent se faire*, répond Lionel Jouneau, maire de Saint-Perreux (Morbihan). *Si on fait appel à des prestataires privés, le coût est exorbitant pour des petits systèmes d'information. Dans les interco, l'échelon est acceptable et il y a des services informatiques.»*

Bon gré ou mal gré, les collectivités vont devoir investir sur la cybersécurité, prévoit Anne Le Henanff. *«On nous pousse à dématérialiser tous nos services, et je suis en faveur de cela*, poursuit-elle. *Mais le problème, c'est qu'il faut absolument que cela s'accompagne d'une sécurisation des matériels et de la sensibilisation de nos agents.»*

**NICOLAS MASSOL**

---

**Suite de la page 2** établissements touchés. *«La situation était d'autant plus critique que l'hôpital avait encore beaucoup de patients Covid*, se souvient ainsi Suzanne Meyer, responsable de la communication de la structure hospitalière d'Albertville-Moûtiers (Savoie), touché en décembre. *Tout est informatisé aujourd'hui, donc on en revient au papier et au crayon. On a récupéré des sauvegardes, on remet en place les dossiers patients, et on réinjecte les données service par service. Tout est à reconstruire.»*

L'autre question, sur le plan moral, est celle du choix de la cible. Pourquoi lancer une cyberattaque contre un hôpital? *«Il faut savoir que ces attaques sont automatisées, ceux qui font ça scannent des plages d'adresses IP en passant de postes en postes. Ils ne savent souvent pas vraiment ce qu'ils attaquent»*, rapporte Baptiste Robert, chercheur en cybersécurité travaillant avec la gendarmerie. Ce que confirment la DGS et l'Anssi. Mais *«dans certains cas, il semble que les attaquants savent qu'ils ont touché une infrastructure de santé»*, ajoutent ces deux institutions.

*«Je suis persuadé qu'avant de rentrer dans les systèmes, ils ne savent pas où ils sont. Mais une fois dedans, c'est très facile de savoir*, poursuit Ivan Fontarensky. *Ils pourraient choisir de ne pas lancer le chiffrement des données. Pendant le premier confinement, un groupe d'attaquants avait justement annoncé avoir annulé une cyberattaque quand ils se sont rendu compte que c'était un hôpital. Le secteur de la santé n'est pas tant ciblé que ça, mais il est vulnérable.»*

**LA SANTÉ, UN SECTEUR TRÈS VULNÉRABLE**

Au-delà des motifs, ces attaques à répétition qui touchent des structures hospitalières, particulièrement sollicitées en pleine pandémie, posent question. Pourquoi, précisément, ces structures si vitales sont-elles vulnérables? *«Les hôpitaux français ne sont pas dans un très bon état de sécurité informatique»*, avance Baptiste Robert. La complexité de ces systèmes informatiques ne joue pas non plus en leur faveur: *«Un hôpital, c'est une ville dans une ville. C'est même extrêmement compliqué de savoir combien il y a d'ordinateurs et de systèmes dans une structure hospitalière, donc forcément c'est beaucoup plus facile d'être un attaquant qu'un défenseur.»*

Les pouvoirs publics en auraient pris conscience, mais les changements sont encore lents. *«Il ne manque pas forcément grand-chose, juste quelques bonnes pratiques*, pointe Ivan Fontarensky. *Mettre à jour les ordinateurs, sensibiliser et faire de la pédagogie sur les pièges comme le phishing* [technique de tromperie pour amener la cible à communiquer ses données personnelles, ndlr]. *Il y a aussi un problème propre au secteur de la santé: les horaires difficiles et la charge de travail rendent compliqué le cloisonnement entre vie personnelle et vie professionnelle, avec parfois l'utilisation du même matériel informatique. Or quand on se fait piéger personnellement, ça peut amener un logiciel malveillant à s'étendre à tout un hôpital.»*

L'enjeu porte également sur l'organisation des systèmes informatiques, comme l'explique Nicolas Arpagian: *«Il va falloir renforcer les politiques de sécurité des hôpitaux, les accompagner. Il faut isoler les systèmes, éviter qu'après une intrusion, on puisse circuler partout. Par exemple, que quelqu'un qui entre par la messagerie puisse accéder aux fichiers des malades, aux plans de rotation des opérations. Investir dans la détection aussi. Mais c'est de la matière grise, du temps, de l'énergie, des moyens. Et c'est rarement la priorité budgétaire des structures hospitalières.»*

Pour le président de la Fédération hospitalière de France, Frédéric Valletoux, qui réagissait mardi sur France Info à la nouvelle cyberattaque contre un établissement de santé, *«les hôpitaux doivent faire partie des cibles protégées au premier niveau, c'est une demande que l'on fait déjà depuis un moment au gouvernement»*.

**«MOINS RISQUÉ QUE LES BRAQUAGES»**

Après l'attaque contre le groupement hospitalier de Villefranche-sur-Saône, la section cybercriminalité du parquet de Paris a lancé mardi une enquête pour *«atteinte à un système de traitement automatisé des données»* et *«tentative d'extorsion en bande organisée»*. Au moins deux autres enquêtes sont ouvertes par cette même section suite aux attaques des CHU de Dax et Albertville-Moûtiers. Pour les mêmes motifs, ainsi que pour *«accès et maintien dans un système de traitement automatisé»*, *«modification des données»*, *«introduction frauduleuse de données»* et *«association de malfaiteurs»*.

Mais derrière ces enquêtes, les arrestations restent rares. Mis à part des coups de filet, comme le démantèlement du réseau international Emotet en janvier ou l'interpellation le 9 février en Ukraine de plusieurs pirates à l'origine du rançongiciel Egregor par les polices ukrainienne, française et le FBI, les auteurs de ces attaques sont difficiles à appréhender. *«Les groupes de cybercriminels sont divisés entre beaucoup de pays, et sont généralement composés de deux à six personnes*, explique Ivan Fontarensky. *On n'est pas forcément face à une organisation, mais à un réseau de développement et d'achat de virus ou de listes d'infrastructures à pirater.»*

Nicolas Arpagian pointe également l'évolution d'une partie de la criminalité traditionnelle vers le piratage: *«C'est rentable et moins risqué que de faire des braquages, les peines sont moindres et l'échelle internationale rend plus difficile le travail des policiers. Les enquêtes nécessitent une vraie coopération entre les pays, il faut trouver des preuves, lister des victimes qui ne se manifestent pas forcément... Des braqueurs peuvent être arrêtés dans la semaine, là ce n'est pas du tout la même temporalité.»* ◆