ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 4267	De **M. Maxime Minot** (Les Républicains - Oise)	**Question écrite**
Ministère interrogé > Intérieur et outre-mer	**Ministère attributaire** > Intérieur et outre-mer	
Rubrique >numérique	**Tête d'analyse** >Accompagnement de l'État contre les cyberattaques	**Analyse** > Accompagnement de l'État contre les cyberattaques.
Question publiée au JO le : **20/12/2022** Réponse publiée au JO le : **27/06/2023** page : **5853**		

Texte de la question

M. Maxime Minot attire l'attention de M. le ministre de l'intérieur et des outre-mer sur les nombreuses cyberattaques que le pays a connu dernièrement. Les dernières cibles datent du début du mois de décembre 2022 : l'hôpital de Versailles ou encore le conseil régional de Normandie ont été attaqués, comme de nombreuses collectivités ou hôpitaux avant eux ces derniers mois. La France n'a jamais connu autant de cyberattaques. Elles ont été multipliées par dix en trois ans seulement. Derrière ces piratages informatiques se trouvent des groupes criminels internationaux très bien organisés. En France, on le sait, les plus actifs sont les *hackers* russophones du groupe « Lockbit ». Une trentaine de cyberattaques d'ampleur leur sont attribuées en 2022, notamment celle commise en septembre 2022 sur le centre hospitalier sud francilien à Corbeil-Essonnes. Ils sont également derrière les vols de données du géant français de l'armement Thalès. La section cyber du parquet de Paris, qui a une compétence sur tout le territoire, a ouvert près de 600 enquêtes pour des attaques cyber depuis le début de l'année 2022 contre seulement 65 il y a trois ans. Parmi toutes ces attaques, celles par rançongiciel sont les plus nombreuses. Elles sont passées de 19 seulement en 2019 à 397 cette année. Les pirates introduisent un logiciel malveillant dans les systèmes informatiques. Ce logiciel crypte les données et les *hackers* réclament ensuite une rançon pour redonner l'accès aux fichiers. Ces rançons peuvent dépasser les 10 millions d'euros. Concernant le centre hospitalier de Corbeil-Essonnes, elle n'a pas été payée et les données de santé de certains patients et membres du personnel ont été dévoilés sur le *dark web*. L'hôpital Mignot de Versailles a d'ores et déjà annoncé qu'il fera de même, la rançon ne sera pas versée. L'établissement, dont les urgences, fonctionne à ce jour toujours en mode dégradé. Les entreprises et les collectivités françaises sont encore mal préparées contre ces prises d'otage informatiques. Il souhaite donc connaître le plan qu'il a prévu pour lutter contre ces cyberattaques par rançongiciel, mais aussi comment il compte accompagner les entreprises, collectivités et les services publics, dans la lutte contre ces menaces.

Texte de la réponse

La loi d'orientation et de programmation du ministère de l'intérieur et des outre-mer constitue la première grande loi numérique du ministère, avec d'importants nouveaux moyens humains, organisationnels et technologiques pour une plus grande efficacité dans la lutte contre la cybercriminalité, un engagement accru dans l'anticipation et la prévention, ainsi qu'un meilleur accompagnement des victimes. Il s'agit en effet d'un enjeu majeur, qui mobilise pleinement les forces de sécurité intérieure de l'État. Les logiciels rançonneurs (dits aussi « rançongiciels ») sont des programmes malveillants chiffrant les données d'ordinateurs à l'insu de leurs utilisateurs, pour afficher un

message indiquant une rançon à verser en échange d'une solution de déchiffrement. Depuis 2018, les pirates recentrent leurs attaques sur les entreprises (pour demander des rançons élevées). Le logiciel malveillant (malware) est injecté parfois plusieurs mois avant le déclenchement du rançonneur. Une exfiltration de données est de plus en plus souvent réalisée, pouvant être suivie d'une diffusion partielle visant à exercer une pression sur la victime. Dans certains cas, le logiciel rançonneur peut aussi être un leurre destiné à masquer des activités d'espionnage (industriel ou étatique). Les logiciels rançonneurs ont démontré leurs capacités destructrices, soit par le nombre de victimes, soit par la sensibilité de leurs cibles. La série d'attaques qui a touché le secteur hospitalier français en 2019, et qui se poursuit, est à la croisée des menaces eu égard à la valeur économique des données et au caractère vital de l'activité hospitalière. La cyberdélinquance est en constante augmentation depuis plusieurs années, avec des taux de progression des faits constatés allant de 10 % à 20 % d'une année sur l'autre selon le type d'infraction. Les attaques par ransomware ont connu une ère d'industrialisation des processus organisationnels des cybercriminels : la méthode de « ransomware as a service » s'est considérablement perfectionnée. Le secteur industriel demeure le plus touché, suivi par les secteurs du commerce et de la santé. Le risque ransomware n'est plus un risque conjoncturel, c'est un risque systémique dont le montant du préjudice peut dépasser le million d'euros en fonction de la taille des structures visées, les cybercriminels adaptant les demandes de rançons à la typologie de leurs cibles. Le commandement de la gendarmerie dans le cyberespace (ComCyberGend) agit sur l'ensemble du spectre missionnel de la gendarmerie dans la lutte contre les cybermenaces. Il agit notamment sur les segments du contact numérique, de la prévention, de la veille des espaces numériques et de l'investigation numérique. Il place ainsi sous une bannière unique l'ensemble du dispositif de lutte contre la cybercriminalité de la gendarmerie nationale et s'appuie sur un réseau territorial de 8 000 cyber-gendarmes intégrés aux échelons territoriaux afin d'apporter une réponse adaptée aux contentieux d'ordre cyber en tout point du territoire, plus particulièrement aux victimes d'attaques par ransomware (rançongiciel). Pour répondre au mieux à cette cybermenace qui touche principalement les entreprises, les collectivités territoriales et les différents organismes publics tels que les établissements de santé, le ComCyberGend a mis en place une capacité d'investigation robuste, adaptable et projetable jusqu'au cœur des territoires. Le ComCyberGend dispose en son sein d'une division des opérations et d'experts techniques de haut niveau. La division des opérations dirige les opérations nationales ou internationales visant les criminalités numériques et assure la direction des opérations pour les enquêtes présentant une particulière gravité ou sensibilité. S'agissant des enquêtes relatives aux ransomwares, elle intervient sous la direction et le contrôle de la section cyber de la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO, Parquet de Paris – section J3). Pour renforcer ses capacités d'investigation, le ComCyberGend s'appuie également sur sa composante expertise numérique et technique qui agit en soutien aux opérations d'investigations numériques et qui peut être sollicitée par tout service d'enquête. Composée de militaires aux compétences de haut niveau, elle apporte une assistance dans les relations avec les entreprises de l'Internet, la projection d'experts pour l'analyse des preuves numériques et le développement d'outils d'enquête pour tous les niveaux de traitement de la délinquance. L'ensemble de ces moyens ne peut être engagé que lorsque l'alerte parvient bel et bien aux enquêteurs. Tel est le sens de l'article 4 de la loi d'orientation et de programmation du ministère de l'Intérieur et des Outre-mer, récemment adoptée par le Parlement, qui encadre les clauses de remboursement des « cyber-rançons » par les assurances. La loi aggrave en outre les peines encourues en cas d'infraction commisse à l'encontre d'un système de traitement automatisé de données. Considérant le développement des offres assurantielles cyber et l'engagement croissant des sociétés de remédiation, il est nécessaire d'encadrer les clauses de remboursement des dommages par les assurances, résultant d'une attaque par rançongiciel. Il s'agit notamment de créer une obligation à la charge des assureurs en conditionnant la prise en charge du sinistre à un dépôt de plainte rapide par la victime. Selon les propos du directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il s'agit bien de ne pas contribuer à l'économie du cybercrime en versant des rançons. Ne pas agir et, donc, de facto, inciter au paiement des rançons revient mécaniquement à rendre plus lucratives ces extorsions et contribue grandement à renforcer une économie du cybercrime. La lutte contre la cyberdélinquance est également une priorité pour la police nationale, qui s'appuie sur un réseau d'enquêteurs spécialisés, aux compétences graduées, mais également sur l'ensemble de ses enquêteurs. La police nationale dispose aujourd'hui de près de 7 000 agents formés à l'investigation sur internet, de 4 600 aux investigations numériques et de près de 10 500 aux investigations en téléphonie. Au-delà, l'ensemble des 23 000 enquêteurs dont disposent les services de la police judiciaire et ceux de

la direction centrale de la sécurité publique (DCSP), avec l'appui des policiers spécialisés, concourent au traitement des enquêtes initiées par les plates formes PHAROS et THESEE (cf. ci-dessous). Pour mener ou assister les enquêtes relatives à des rançonneurs, tous les policiers disposent, dans le logiciel de rédaction des procédures de la police nationale, de modèles de procès-verbaux de plainte et d'audition de victime et d'une fiche réflexe conçus par le tribunal judiciaire de Paris (section J3). La sous-direction de la lutte contre la cybercriminalité (SDLC) de la Direction centrale de la police judiciaire (DCPJ) est chargée du pilotage et de la coordination de la lutte contre ce phénomène. Le 3 février 2020, la section spécialisée cyber du parquet du tribunal judiciaire de Paris a affirmé le rôle centralisateur de cette sous-direction de la lutte contre la cybercriminalité et arrêté le principe de sa co-saisine systématique pour toutes les familles de logiciels rançonneurs. La SDLC dispose d'un Office central de lutte contre la criminalité liée aux technologies de l'information et de la communicatio (OCLCTIC). Cet office met en œuvre un dispositif complet de lutte contre la cyberdélinquance et anime et coordonne, au niveau national, la mise en œuvre opérationnelle de la lutte contre la cybercriminalité. L'OCLCTIC inclut par ailleurs des brigades judiciaires spécialisées dont l'action se focalise notamment sur les atteintes aux systèmes de traitement automatisé de données et les offres de cyber services criminels (forums du darkweb, solutions de téléphonie chiffrée, etc.). Elles sont appuyées par une division de l'anticipation et de l'analyse qui recherche et croise, en liaison étroite avec les acteurs de la sécurité informatique du secteur privé, les éléments techniques permettant d'identifier l'origine des attaques (base de données MISP-PJ, commune à la police nationale et à la gendarmerie nationale). Le dispositif comprend également la plate-forme PHAROS (plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), une brigade judiciaire, et la plate-forme THESEE (traitement harmonisé des enquêtes et des signalements pour les e-escroqueries). Par ailleurs, en sa qualité d'office central, l'OCLCTIC est le point de contact national de la coopération européenne et internationale. Ce rôle est fondamental en matière de lutte contre la cybercriminalité. L'office est également le représentant français à la task-force resserrée d'Europol dédiée à la lutte contre la cybercriminalité. Enfin, l'OCLCTIC participe de longue date aux actions opérationnelles menées dans le cadre des priorités du « cycle politique européen ». La sous-direction de la lutte contre la cybercriminalité dispose également d'un bureau de l'aide à l'enquête numérique, chargé de développer des canaux de communication avec les fournisseurs de services sur internet. Intégré à la SDLC, un CSIRT-PJ (Computer Security Incident Response Team) fait le lien avec la communauté des centres d'alerte cyber. Enfin, la sous-direction de la lutte contre la cybercriminalité a mis en place en 2018 un réseau cybermenaces (RCM) destiné à améliorer la conscience des risques cyber par les acteurs du tissu économique local et des enjeux des enquêtes judiciaires en cas d'attaque (nécessité d'un dépôt de plainte, impérieuse conservation des données techniques utiles aux enquêteurs…). Il vise en premier lieu les TPE/PME, particulièrement vulnérables. Depuis septembre 2020, la DCSP anime pour sa part un partenariat avec le réseau des directeurs de la sécurité du groupe Agora Managers, autour des menaces identifiées par le renseignement territorial (RT) en matière de sécurité économique et de prévention de la radicalisation. En complément, afin de proposer aux petites et moyennes entreprises ou aux collectivités territoriales des actions de prévention incluant la cyber-délinquance, une initiative conjointe des référents sûreté de la DCSP et des référents cyber-menaces de la DCPJ a été mise en place depuis mai 2022 : ces spécialistes animent ensemble, à la demande de collectivités territoriales et d'acteurs économiques publics et privés, des séances de sensibilisation à la sûreté et à la cybersécurité. 16 laboratoires d'investigation opérationnelle du numérique (LION), déployés dans les services territoriaux de la DCPJ et à la préfecture de police, structurent également le dispositif local et permettent la mutualisation d'outils et de compétences. La sous-direction de la lutte contre la cybercrminalité de la DCPJ entretient également des partenariats avec de nombreuses institutions et sociétés, tant pour mieux prendre en compte les victimes que pour leur permettre de mieux anticiper les menaces. Des liens sont aussi développés avec des entreprises de cybersécurité. La lutte contre les logiciels rançonneurs constitue, naturellement, une priorité de l'action de la sous-direction de la lutte contre la cybercriminalité, qui déploie un dispositif global pour faire le lien entre l'ensemble des acteurs, privés et publics, en interface avec les structures de coopération internationale policière. Elle organise la convergence de l'ensemble des capteurs, dans une démarche de renseignement criminel directement tournée vers la détermination d'objectifs opérationnels. Il s'agit aussi de favoriser la remontée d'une information structurée. La démarche d'investigation systématique menée par la police judiciaire vise à casser le sentiment d'impunité qui favorise l'émergence de nouveaux groupes criminels. La convergence de l'action judiciaire permet l'identification de groupes criminels à l'origine des attaques. Les résultats obtenus en 2020 et en 2021 sur

des affaires majeures valident cette stratégie (affaires Egregor, LockerGaga….). La SDLC s'attache également à démanteler les structures support d'un écosystème cybercriminel basé sur une offre de sous-traitance (« crime-as-a-service »).