ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 38319	De **M. Christophe Blanchet** (Mouvement Démocrate (MoDem) et Démocrates apparentés - Calvados)	**Question écrite**
Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Première ministre	
Rubrique >numérique	**Tête d'analyse** >État de la menace « rançongiciel » en France	**Analyse** > État de la menace « rançongiciel » en France.

Question publiée au JO le : **20/04/2021**
Réponse publiée au JO le : **21/06/2022** page : **3361**
Date de changement d'attribution : **17/05/2022**
Date de renouvellement : **03/08/2021**
Date de renouvellement : **04/01/2022**
Date de renouvellement : **26/04/2022**

Texte de la question

M. Christophe Blanchet alerte M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur le phénomène du rançongiciel ou *ransomware* qui consiste, pour un individu ou un groupe mal intentionné, à « prendre en otage » les données d'une organisation, d'une entreprise ou encore d'un particulier à l'aide d'un logiciel malveillant. Le rançongiciel chiffre et bloque les fichiers contenus sur le réseau informatique et demande une rançon en échange du moyen de les déchiffrer. Depuis peu, le rançongiciel exfiltre préalablement les données en vue d'une future divulgation ou vente aux enchères. La finalité est de faire chanter la victime contre une somme d'argent à payer le plus souvent par cryptomonnaie. L'entreprise spécialisée en *blockchains* Chainalysis estime, après analyse des seules transactions par cryptomonnaie, qu'en 2020, au moins 350 millions de dollars auraient été versés dans le monde par les victimes de rançongiciels, quatre fois plus qu'en 2019. Par ailleurs, en Allemagne, une femme est décédée dans la nuit du 11 au 12 septembre 2020, et l'une des causes de son décès pourrait être un rançongiciel. En effet, la personne a dû être transportée en urgence absolue vers l'hôpital universitaire de Düsseldorf. L'établissement n'a pas pu l'accueillir, car un rançongiciel avait bloqué son système d'information. La menace rançongiciel pèse en France avec une intensité qui croît de manière inédite et préoccupante. Elle capte des montants considérables au profit de l'écosystème cybercriminel, et entraîne des préjudices concrets dans la vie quotidienne. Selon le rapport de l'ANSSI sur l'état de la menace rançongiciel, les collectivités locales seraient préférentiellement ciblées pour leur propension à payer la rançon. Aux États-Unis d'Amérique, la *Cybersecurity and Infrastructure Security Agency* (CISA) a lancé en janvier 2021 une campagne inter-administration en coopération avec le secteur privé pour réduire le risque lié aux rançongiciels. Il lui demande, pour les entreprises et les administrations françaises, quelle est l'estimation du montant total versé par les victimes de rançongiciels ? Quels ont été les impacts des rançongiciels en France sur la vie quotidienne des Français, alors même que de nombreux hôpitaux français ont été touchés en 2020, en contexte de pandémie ? Enfin, en France, il lui demande quelle politique publique d'évaluation, de prévention et de réduction de la menace rançongiciel est mise en œuvre, notamment à destination des services au public.

Texte de la réponse

La menace représentée par les rançongiciels touche l'ensemble de notre société et affecte indéniablement le quotidien de nos concitoyens, a fortiori s'agissant des incidences sur les collectivités territoriales et les établissements hospitaliers qui sont particulièrement visés. En conséquence, le Gouvernement a fait le choix stratégique de doter France Relance d'un volet consacré au renforcement de la cybersécurité. Pour ce faire, une première enveloppe de crédits a été fixée à 136 M€. Elle a été complétée de 40 M€ supplémentaires en 2022. L'objectif stratégique poursuivi est avant tout de hausser le niveau de sécurité numérique de l'Etat et des services publics. Les actions mises en place sont donc destinées aux collectivités territoriales, aux établissements de santé, aux autres établissements publics et aux institutions publiques, parmi lesquelles les ministères. Outre l'accélération de la mise en œuvre de nouveaux services de cybersécurité pour les agents et réseaux de l'Etat, plusieurs dispositifs sont accessibles aux collectivités territoriales, parmi lesquels le soutien à la création de centres territoriaux de réponse à incident de cybersécurité. Ces projets, portés par les conseils régionaux, permettront d'apporter une réponse concrète à toutes les victimes de cyberattaques sur l'ensemble du territoire considéré. Au printemps 2022, dix régions métropolitaines se sont déjà vues accorder un soutien financier d'un million d'euro chacune pour créer un centre régional de réponse à incident. Parmi elles, sept suivent actuellement un programme d'incubation qui permettra de rendre ces structures opérationnelles d'ici la fin de l'année 2022. D'autres régions devraient incessamment se déclarer candidates à la création de centre de réponse à incident. Elles suivront un programme d'incubation similaire au second semestre. Le Gouvernement espère que l'ensemble des régions s'engagera in fine dans cette démarche. Il convient de signaler que ce dispositif a vocation à être pleinement adopté dans les outre-mer. Des discussions sont en cours pour adapter les structures aux spécificités géographiques ou économiques de ces territoires. D'ici l'été 2022, plusieurs projets seront soutenus, par zone géographique. Il s'agira de faire émerger un tissu de prestataires locaux en cybersécurité capables d'œuvrer en matière de prévention, de sécurisation et de réponse à incidents, de diffuser les bonnes pratiques en les adaptant aux contextes locaux et de faire émerger des offres de formation locales. Enfin, au-delà du soutien à la création de ces structures, en métropole ou en outre-mer, l'enjeu réside dans leur pérennisation : le modèle de fonctionnement devra prendre en compte le service rendu aux acteurs locaux et assurer auprès des victimes sa mission de réponse de premier niveau en cas d'attaque. Ces structures pourront également proposer des prestations pertinentes et à forte valeur ajoutée pour le tissu économique local et initier ainsi des collaborations étroites avec les fédérations locales, les conseils régionaux et départementaux, les chambres de commerces et les secteurs industriels locaux.