ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 45367	De **Mme Josiane Corneloup** (Les Républicains - Saône-et-Loire)	**Question écrite**

Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Économie, finances, souveraineté industrielle et numérique

Rubrique >Internet	**Tête d'analyse** >Hausse des cybermalveillances	**Analyse** > Hausse des cybermalveillances.

Question publiée au JO le : **26/04/2022**
Date de changement d'attribution : **21/05/2022**
Question retirée le : **21/06/2022** (fin de mandat)

Texte de la question

Mme Josiane Corneloup appelle l'attention de 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 la hausse des cybermalveillances. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) et cybermalveillance.gouv.fr constatent que les cyberattaques sont de plus en plus nombreuses dans leurs rapports annuels, ils dressent un état des lieux des principales menaces observées en 2021. Hameçonnage, piratage de compte, rançongiciels, violation de données, etc. : la liste est très longue ! Cybermalveillance.gouv.fr constate une hausse importante des demandes d'assistance en ligne. Cette plateforme d'aide aux victimes de cybercriminalité a enregistré plus de 173 000 demandes en 2021, soit plus 65 % par rapport à 2020. De son côté, l'ANSSI a également publié un « panorama de la menace informatique » qui fait état de 1 082 intrusions avérées dans des systèmes d'information en 2021, contre 786 en 2020, soit une augmentation de 37 %. Ces nombreuses cyberattaques ont des finalités diverses : gains financiers, espionnage, déstabilisation, sabotage, etc. Sur les 47 formes de cybermalveillance relevées par la plateforme cybermalveillance.gouv.fr, l'hameçonnage est la principale menace rencontrée tous publics confondus, qu'il s'agisse des particuliers, des entreprises ou des collectivités. Cette technique d'attaque consiste à envoyer un *mail* ou un SMS à la victime pour l'inciter à communiquer des informations personnelles ou bancaires en usurpant l'identité d'un tiers de confiance. Le piratage de compte en ligne représente la deuxième menace constatée par la plateforme avec une augmentation de 139 % en 2021. Au total, près de 160 000 personnes ont cherché de l'aide sur ce phénomène. Si le piratage des comptes bancaires en ligne ou des comptes de réseaux sociaux restent principalement visés, les cybercriminels s'intéressent de plus en plus aux comptes de messageries. Les utilisateurs y conservent une grande quantité d'informations, documents d'identité, fiches de paie, avis d'imposition qui peuvent être dérobées pour mener, par exemple, des usurpations d'identité afin de contracter un crédit. Les consultations au sujet des rançongiciels sont également en forte hausse (+ 95 %), elles tiennent la première place des menaces auprès des entreprises et des collectivités, selon le rapport de cybermalveillance.gouv.fr. Ces logiciels, qui bloquent l'accès aux systèmes informatiques de la victime jusqu'au paiement d'une rançon, ciblent principalement les entreprises. Celles-ci seraient, en effet, plus enclines à payer les rançons demandées pour éviter les impacts économiques et réputationnels sur leur activité. D'après l'ANSSI, ces attaques particulièrement lucratives pour les cybercriminels peuvent aussi être réalisées par des acteurs étatiques à des fins de déstabilisation, de sabotage ou d'espionnage informatique. En conséquence, elle lui demande de bien vouloir lui préciser quelles sont les actions que le Gouvernement va entreprendre afin de sécuriser les entreprises, les collectivités et les particuliers contre les cybermalveillances dont le nombre ne cesse de croître.

ASSEMBLÉE NATIONALE