ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 38078	De **M. Bastien Lachaud** (La France insoumise - Seine-Saint-Denis)	**Question écrite**

Ministère interrogé > Éducation nationale, jeunesse et sports	**Ministère attributaire** > Éducation nationale, jeunesse et sports

Rubrique >Internet	**Tête d'analyse** >Attaques informatiques sur les ENT scolaires	**Analyse** > Attaques informatiques sur les ENT scolaires.

Question publiée au JO le : **13/04/2021**
Réponse publiée au JO le : **08/03/2022** page : **1558**

Texte de la question

M. Bastien Lachaud interroge M. le ministre de l'éducation nationale, de la jeunesse et des sports sur les éventuelles attaques informatiques étrangères contre la plateforme « Ma classe à la maison ». M. le ministre a en effet avancé que les déboires connus le 6 avril 2021 par les utilisateurs de ce service trouveraient en grande partie leur origine dans des attaques informatiques venues de l'étranger. Si tel est le cas, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et l'Agence nationale de la sécurité des systèmes d'information placés sous l'autorité du Premier ministre seront certainement en mesure de fournir un rapport précis. *A contrario*, il serait inconcevable qu'un ministre puisse mentir et prendre à la légère un sujet aussi grave que la sécurité informatique et la vulnérabilité de l'État aux attaques cyber. Celles dont ont par exemple été victimes différents hôpitaux ces derniers mois devraient inciter à mesurer la gravité des enjeux et à faire preuve d'une grande retenue. C'est pourquoi il souhaite savoir si les services compétents ont effectivement détecté des attaques informatiques d'ampleur, d'origine étrangère, contre la plateforme « Ma classe à la maison » et quelles sont les caractéristiques techniques de ces éventuelles attaques.

Texte de la réponse

Entre le 6 et le 9 avril, la plate-forme Ma Classe à la Maison (MACLAM) a été fortement impactée par des attaques employant des moyens très professionnels pour déstabiliser le dispositif de continuité pédagogique. Des ralentissements ont été ressentis le matin, parfois des inaccessibilités du fait de la longueur du temps de réponse. Selon l'avis de l'hébergeur et l'opérateur : « il s'agit d'attaques sur-mesure réalisées par des personnes expérimentées et disposant de moyens particulièrement importants ». Ces deux acteurs se sont fortement mobilisés pendant la semaine pour limiter l'impact de ces attaques sans pouvoir empêcher que des ralentissements importants surviennent à plusieurs reprises devant l'ampleur des moyens déployés (volume et diversité des techniques d'attaque). Il est impossible pour le CNED de communiquer les informations techniques relatives à ces attaques puisqu'une enquête est ouverte et que chaque élément technique constitue une preuve qui ne sera recevable que si elle respecte un processus strict de communication aux autorités. Pour ce qui concerne les éléments ou indices probants, les prestataires du CNED font état d'un nombre anormalement élevé de requêtes illégitimes. Les sollicitations sur les serveurs ont été 100 à 1 000 fois supérieures au nominal que ce soit sur une adresses IP, un serveur, un port, reflétant ainsi une volonté délibérée de surcharger et faire tomber les services. Ces attaques ont utilisé des stratégies changeantes, s'en prenant tantôt aux aspects réseaux, tantôt aux applicatifs, en modifiant les algorithmes à chaque fois qu'une parade était mise en place par l'opérateur internet ou l'hébergeur. L'ensemble des

attaques à ce jour répertoriées sont des attaques par déni de service et ne remettent pas en cause l'intégrité des plateformes et des données. Par rapport à l'an dernier, les volumes des attaques sont considérablement plus élevés et les techniques mises en œuvre plus élaborées, comme le soulignent les prestataires spécialisés qui doivent affronter ces situations de crise. Pour avoir une idée de l'ampleur des attaques, l'une des attaques subie lors de la nuit du 6 au 7 avril avait la capacité de générer plus de 300 Go de données en simultané sur le serveur d'entrée alors que la moyenne est de quelques dizaines de Go en simultané pour un hébergeur et ce pour l'ensemble de ses services.