Ministère
de l'Environnement
et de la Lutte contre
les changements
climatiques
Québec

Direction des renseignements, de l'accès à l'information
et des plaintes sur la qualité des services

Québec, le 29 octobre 2018

Objet : Demande d'accès n° 2018-10-046 – Lettre réponse

Madame,

La présente fait suite à votre demande d'accès, reçue le 17 octobre dernier, concernant tous les rapports et autres documents portant sur les intrusions et hameçonnages informatiques réussis dans le réseau du Ministère, ainsi que sur les tentatives d'intrusions et d'hameçonnages informatiques bloquées depuis 2014.

Le document suivant est accessible. Il s'agit de :

1. Hameçonnages et intrusions réussis depuis 2014, 1 page.

Conformément à l'article 51 de la Loi, nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information. Vous trouverez, en pièce jointe, une note explicative concernant l'exercice de ce recours.

Pour obtenir des renseignements supplémentaires, vous pouvez joindre M^me^ Marie-Eve Gravel-Nadon, analyste responsable de votre dossier, à l'adresse courriel marie-eve.gravel-nadon@mddelcc.gouv.qc.ca, en mentionnant le numéro de votre dossier en objet.

Veuillez agréer, Madame, l'expression de nos sentiments les meilleurs.

La directrice,

ORIGINAL SIGNÉ PAR

Pascale Porlier

p. j. (2)

Édifice Marie-Guyart, 29e étage
675, boul. René-Lévesque Est, boîte 13
Québec (Québec) G1R 5V7
Téléphone : 418 521-3858
Télécopieur : 418 643-0083
Courriel : acces@mddelcc.gouv.qc.ca
Internet : www.mddelcc.gouv.qc.ca

Ministère
de l'Environnement
et de la Lutte contre
les changements
climatiques
Québec

En ce qui concerne les hameçonnages et intrusions réussis depuis 2014, nous n'avons observé aucun cas au Ministère.

En ce qui concerne les tentatives de hameçonnage et les tentatives d'intrusions bloquées.

- l'antivirus a bloqué :
    - Cheval de Troie : 1475 (dont 67 cas spécifiques de hameçonnage)
    - Virus : 2
    - Programmes potentiellement indésirables : 22
    - Canulars : 2
- La sonde réseau au périmètre a bloqué
    - Corruption de mémoire : 15
    - Dépassement de tampon (Buffer Overflow) : 62
    - Exploit Kits : 23
    - Exécution de code : 2
    - Shell malicieux : 1

Notes :

1. Le journal antivirus ne rapporte que les événements des six derniers mois;
2. Le journal de la sonde réseau au périmètre rapporte les événements pour les 17 derniers mois seulement;
3. Les métriques ci-dessus ne représentent pas des attaques distinctes, il s'agit plutôt d'un nombre d'événements journalisé par catégories, étant donné qu'une attaque peut générer plusieurs événements;
4. De plus, ces métriques ne sont pas nécessairement exclusives qu'à des cas d'intrusions.