Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2025-143

Version PDF

Gatineau, le 13 juin 2025

Dossier public : 1011-NOC2025-0143

Appel aux observations – Modifications proposées au cadre pour limiter le trafic des réseaux de zombies

Date limite de dépôt des interventions : 14 juillet 2025

Date limite de dépôt des répliques : 29 juillet 2025

[Soumettre une intervention ou voir les documents connexes]

Sommaire

Le Conseil aide à assurer que la population canadienne ait accès à des services de télécommunication sécuritaires et fiables grâce à ses activités réalisées en vertu de la *Loi sur les télécommunications* (*Loi*) et de la *Loi canadienne anti-pourriel* (LCAP). En vertu de la *Loi*, il joue un rôle restreint en réglementant les fournisseurs de services de télécommunication (FST). En vertu de la LCAP, il aide à protéger la population canadienne des messages indésirables en ligne, de concert avec le Bureau de la concurrence Canada et le Commissariat à la protection de la vie privée du Canada, en promouvant et en surveillant la conformité par le biais d'un régime de réglementation civil.

Un réseau de zombies est un réseau d'ordinateurs, de téléphones cellulaires ou d'autres appareils été infectés par des logiciels malveillants. Cela permet à des individus ou à des groupes de contrôler les appareils à l'insu et sans le consentement de leurs propriétaires. Les réseaux de zombies peuvent être utilisés pour envoyer des pourriels à la population canadienne ou pour d'autres activités néfastes. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170, le Conseil a conclu que des mesures réglementaires étaient nécessaires afin que les FST aident à démanteler les réseaux de zombies et à protéger la population canadienne des dommages qu'ils causent. Dans cette décision, le Conseil a précisé les lignes directrices d'un cadre de réglementation en vue de bloquer les activités malveillantes des réseaux de zombies.

Dans la décision de Conformité et Enquêtes et de Télécom 2025-142, le Conseil a établi un cadre qui énonce les modalités pour permettre aux entreprises canadiennes de bloquer les réseaux de zombies et d'autres activités néfastes au sein de leurs réseaux avant qu'ils n'atteignent les appareils de la population canadienne. Actuellement, le cadre ne permet que l'utilisation de listes de blocage.

Canada

Dans le présent avis de consultation le Conseil recueille des points de vue à savoir si la portée du cadre devrait être élargie pour inclure d'autres méthodes de blocage

Contexte

1. Dans la décision de Conformité et Enquêtes et de Télécom 2025-142, le Conseil a établi un cadre qui définit les modalités permettant aux entreprises canadiennes de bloquer les réseaux de zombies et d'autres activités néfastes à l'échelle des réseaux avant qu'ils n'atteignent les appareils de la population canadienne. Actuellement, le cadre ne permet que l'utilisation de listes de blocage. Les listes de blocage sont des listes de renseignements qui aident à repérer les activités néfastes. Les entreprises peuvent utiliser ces listes pour empêcher le trafic en ligne suspect ou dangereux de passer par leurs réseaux.

2. Le Conseil envisage d'élargir la portée du cadre final pour inclure d'autres méthodes de blocage, comme celles basées sur les signatures de fichiers, les anomalies de volume de trafic et les empreintes digitales du réseau. Étant donné que le Conseil dispose actuellement de peu de renseignements sur ces autres méthodes de blocage, il amorce la présente consultation publique afin de recueillir des observations sur la possibilité et la manière de les intégrer au cadre et, s'il y a lieu, sur la nécessité d'ajouter d'autres mesures de protection de la vie privée et exigences en matière de production de rapports.

Appel aux observations

3. Le Conseil accueille favorablement les observations sur les questions ci-dessous. Les intéressés sont invités à répondre aux questions les plus pertinentes pour eux et ne sont pas tenus de répondre à toutes les questions. Des définitions et des rapports qui peuvent aider les parties à préparer leurs répliques sont énumérés dans l'annexe du présent avis.

Utilisation actuelle ou prévue par les entreprises canadiennes de méthodes de blocage différentes de celles décrites à la section 2 du cadre

4. Le Conseil recueille de l'information au sujet du fonctionnement des méthodes de blocage des entreprises canadiennes. Les opinions de toutes les parties à ce sujet sont les bienvenues. Ces renseignements aideront le Conseil à déterminer si davantage de méthodes devraient être autorisées et, s'il y a lieu, sous quelles conditions.

Q1. Utilisez-vous le blocage de port ou prévoyez-vous le faire? Dans l'affirmative, quels ports ou protocoles sont ou seraient bloqués?

Q2. Bloquez-vous le trafic Internet qui inclut une fausse adresse source, ou prévoyez-vous le faire? Dans l'affirmative, quelles procédures utilisez-vous ou prévoyez-vous utiliser pour déterminer s'il s'agit d'une fausse adresse de protocole Internet (IP) source?

Q3. Bloquez-vous ou prévoyez-vous bloquer le trafic Internet en fonction des signatures de fichiers?

i) Dans l'affirmative, quels indicateurs sont, ou seraient, utilisés pour détecter et bloquer le trafic Internet à l'aide de cette méthode (p. ex. des hachages cryptographiques de binaires ou de scripts malveillants, ou des certificats de signature de code dans les binaires)?

ii) D'où viennent ces indicateurs (p. ex. listes de blocage internes ou de tiers)?

iii) Cette méthode de blocage devrait-elle être intégrée à une liste de blocage et, dans l'affirmative, faut-il apporter des ajustements au cadre (p. ex. à la définition de l'indicateur de compromission ou aux exigences applicables à l'utilisation des listes de blocage)?

Q4. Bloquez-vous ou prévoyez-vous bloquer le trafic Internet en fonction des anomalies de volume de trafic afin de prévenir les attaques volumétriques?

Q5. Utilisez-vous d'autres méthodes de blocage à l'échelle des réseaux qui ne sont pas mentionnées dans les questions précédentes (p. ex. méthodes basées sur les empreintes digitales du réseau), ou prévoyez-vous le faire? Dans l'affirmative, décrivez chacune de ces autres méthodes.

Questions sur la protection de la vie privée liées à toutes les méthodes de blocage

Q6. Dans le cadre de la surveillance des points de données pour le blocage à l'échelle des réseaux, avez-vous recours à l'inspection approfondie des paquets ou à d'autres techniques similaires?

i) Dans l'affirmative, est-ce que seuls les en-têtes de paquets sont inspectés ou est-ce que le contenu des communications est également inspecté (lorsqu'il n'est pas chiffré)?

ii) Quels points de données sont inspectés à l'aide de l'inspection approfondie des paquets en vue de détecter et de bloquer le trafic Internet malveillant?

Q7. Pour toute méthode de détection et de blocage, est-ce que des renseignements personnels sont recueillis, enregistrés ou conservés sur des points de contrôle de réseau ou autrement?

i) Dans l'affirmative, quelle est la période de conservation et qui a accès aux renseignements personnels?

ii) Comment ces renseignements personnels sont-ils utilisés et communiqués?

iii) Si ces renseignements personnels sont groupés et dépersonnalisés, comment sont-ils utilisés et communiqués?

Ajout de mesures de protection au cadre pour aider à protéger la vie privée

Q8. Devrait-on interdire aux entreprises qui utilisent des méthodes de blocage autres que les listes de blocage d'examiner, d'analyser ou de conserver le contenu des communications électroniques? Dans l'affirmative, pourquoi?

Q9. Devrait-on interdire aux entreprises d'utiliser ou de communiquer les renseignements recueillis par l'intermédiaire du cadre (p. ex. volume de trafic d'un ménage ou sites Web visités) à d'autres fins (p. ex. publicité ciblée)? Dans l'affirmative, pourquoi?

Q10. Devrait-on interdire aux entreprises de conserver les renseignements sur les en-têtes des paquets ou de conserver ces renseignements au-delà d'une période acceptable? Dans l'affirmative, pourquoi?

Ajout au cadre d'obligations en matière de production de rapports si des méthodes de blocage supplémentaires sont autorisées

Q11. Si le Conseil décide d'autoriser l'une ou l'autre des méthodes de blocage énumérées dans les questions Q1 à Q5, devrait-il modifier les exigences en matière de production de rapports du cadre afin d'améliorer la transparence de l'efficacité des méthodes de blocage des entreprises (p. ex. statistiques sur le blocage par signature)?

Q12. Sachant que le Conseil souhaite que le cadre soit souple et neutre sur le plan technologique et souple, les entreprises devraient-elles être invitées à déclarer annuellement leurs méthodes de blocage? Si vous n'êtes pas d'accord, veuillez expliquer pourquoi.

Ce qu'il faut savoir pour participer à la présente instance

Procédure

5. Les *Règles de pratique et de procédure du Conseil de la radiodiffusion et des télécommunications canadiennes* (*Règles de procédure*) s'appliquent à la présente instance. Les Lignes directrices à l'égard des *Règles de pratique et de procédure du CRTC* (bulletin d'information de radiodiffusion et de télécom 2010-959) ont pour but d'aider le public à comprendre les *Règles de procédure* afin qu'il puisse participer plus efficacement aux instances du Conseil.

6. Le Conseil encourage les réponses, entre autres, des entreprises de services locaux titulaires et concurrentes, des fournisseurs, des fournisseurs de système de noms de domaine de protection, des sociétés d'hébergement Web et des organisations gouvernementales dont le mandat comprend la protection des infrastructures essentielles, des réseaux informatiques ou des renseignements personnels.

Déposer des interventions et des répliques

7. Le Conseil invite les intéressés à déposer des observations au sujet des enjeux et des questions identifiés ci-dessus. Il acceptera les interventions reçues au plus tard le **14 juillet 2025**.

8. Les intéressés qui ont besoin d'aide pour déposer leurs observations peuvent communiquer avec le groupe des audiences et des instances publiques du Conseil à audience@crtc.gc.ca.

9. Les intéressés qui souhaitent déposer une intervention deviennent automatiquement parties à la présente instance. Seules les parties à l'instance peuvent participer aux étapes ultérieures de l'instance. La date limite pour le dépôt des répliques est le **29 juillet 2025**. Les répliques peuvent porter sur toute question figurant dans le dossier de l'instance.

10. Les mémoires doivent être déposés auprès du secrétaire général du Conseil au moyen de l'une des façons suivantes :

    - en remplissant le formulaire d'intervention du Conseil;
    - en envoyant une télécopie au 819-994-0218;
    - en écrivant par courrier à l'adresse suivante : CRTC, Gatineau (Québec) K1A 0N2.

11. Les mémoires de plus de cinq pages devraient inclure un résumé. Les mémoires seront affichés dans la langue et le format officiels dans lesquels ils ont été reçus.

12. L'heure limite de dépôt des interventions au Conseil est fixée à 17 h, heure de Vancouver (20 h, heure de Gatineau). Les parties doivent veiller à ce que leurs mémoires soient déposés en temps opportun. Elles ne seront pas informées si leurs mémoires sont reçus après la date limite. Les mémoires déposés en retard ne seront pas pris en compte par le Conseil et ne seront pas versés au dossier public.

Avis de confidentialité

13. Veuillez porter attention aux points suivants :

    - Les documents seront affichés sur le site Web du Conseil exactement comme ils ont été reçus. Ces documents comprennent tous les renseignements personnels qu'ils contiennent, tels que le nom complet, le courriel, l'adresse postale et les numéros de téléphone et de télécopieur.
    - Tous les renseignements personnels que les parties fournissent dans le cadre de la présente instance publique, à l'exception des renseignements désignés comme confidentiels, seront affichés sur le site Web du Conseil et pourront être consultés par d'autres personnes.

- Toutefois, les renseignements que les parties fournissent ne peuvent être consultés qu'à partir de la page Web de cette instance publique. Par conséquent, une recherche généralisée du site Web du Conseil, à l'aide de son moteur de recherche ou de tout autre moteur de recherche, ne permettra pas d'accéder directement aux renseignements fournis dans le cadre de ce processus public.

- Les renseignements personnels fournis par les parties peuvent être divulgués et seront utilisés aux fins auxquelles ils ont été recueillis ou compilés par le Conseil, ou pour un usage qui est compatible avec ces fins.

Confidentialité

14. Les instances du Conseil sont conçues pour permettre au public d'apporter sa contribution afin que le Conseil puisse prendre de meilleures décisions plus éclairées. Par conséquent, la règle générale est que tous les renseignements déposés auprès du Conseil sont versés au dossier public et peuvent être examinés par toutes les parties et le public.

15. Cependant, le Conseil a souvent besoin de renseignements détaillés de la part des entreprises qu'il réglemente et supervise pour prendre une décision éclairée. Ces renseignements peuvent être de nature confidentielle sur le plan commercial, d'autant plus que l'environnement dans lequel les entreprises exercent leurs activités devient de plus en plus concurrentiel. Le Conseil acceptera donc de considérer certains renseignements confidentiels.

16. Les parties peuvent demander que ces renseignements soient déposés à titre confidentiel en vertu du paragraphe 39(1) de la *Loi sur les télécommunications*, avec une justification détaillée des raisons pour lesquelles ces renseignements devraient être considérés confidentiels. Le Conseil rappelle aux parties qui font une telle demande que lorsqu'un document contenant des renseignements confidentiels est déposé, une version abrégée doit également être déposée afin d'être incluse dans le dossier public.

Formats accessibles aux personnes handicapées

17. Le Conseil exige que, pour la présente instance, les entités réglementées déposent leurs mémoires dans des formats accessibles (p. ex. des formats de fichier texte dont le texte peut être agrandi ou modifié, ou lu par un lecteur d'écran) et il encourage toutes les parties à faire de même. Pour leur faciliter la tâche, le Conseil a affiché sur son site Web des lignes directrices pour la préparation des documents en formats accessibles.

18. Dans le cas où un document n'aurait pas été déposé dans un format accessible, vous pouvez communiquer avec le groupe des audiences et des instances publiques du Conseil à l'adresse électronique audience@crtc.gc.ca pour demander au personnel du Conseil d'obtenir ce document dans un format accessible auprès de la partie qui l'a initialement déposé.

Accéder aux documents

19. On peut accéder aux interventions, ainsi qu'à d'autres documents dont il est question dans le présent avis, en cliquant sur les liens dans la page Consultations et audiences : donnez votre avis du Conseil.

20. Les documents sont disponibles sur demande, pendant les heures normales de bureau. Veuillez contacter :

    Centre de documentation
    Examinationroom@crtc.gc.ca
    Tél. : 819-997-4389
    Téléc. : 819-994-0218

    Service à la clientèle
    Téléphone sans frais : 1-877-249-2782
    ATS sans frais : 1-877-909-2782

21. Les intéressés peuvent trouver les versions électroniques des documents en cliquant sur « [Soumettre une intervention ou consulter les documents connexes] » dans le haut du présent avis.

Secrétaire général

Documents connexes

- *Développement d'un cadre pour limiter le trafic des réseaux de zombies*, Décision de Conformité et Enquêtes et de Télécom CRTC 2025-142, 13 juin 2025

- *Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens*, Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170, 23 juin 2022; modifiée par la décision de Conformité et Enquêtes et de Télécom CRTC 2022-170-1, 11 octobre 2022

- *Lignes directrices à l'égard des Règles de pratique et de procédure du CRTC*, Bulletin d'information de radiodiffusion et de télécom CRTC 2010-959, 23 décembre 2010

Annexe à l'Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2025-143

Blocage de ports

Voir le document intitulé Port Blocking, Broadband Internet Technical Advisory Group, août 2013 [en anglais seulement].

Le blocage du trafic SMTP [Simple Mail Transfer Protocol] sur le port 25, par exemple, est une pratique courante qui permet de prévenir les pourriels, comme il est recommandé dans les rapports suivants :

- Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction, Messaging Anti-Abuse Working Group, 2005 [en anglais seulement]

- Recommended Internet Service Provider Security Services and Procedures, Request for Comments (RFC) 3013, Tom Killalea, Internet Engineering Task Force (IETF), novembre 2000 (RFC 3013) [en anglais seulement]

Les documents ci-dessous indiquent également que les entreprises utilisent efficacement cette pratique :

- Paragraphes 52 et 53 de la *Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens*, décision de Conformité et Enquêtes et de Télécom CRTC 2022-170, 23 juin 2022; modifiée par la décision de Conformité et Enquêtes et de Télécom CRTC 2022-170-1, 11 octobre 2022

- Mesures anti-pourriel du FSI contestées, Résumé de conclusions d'enquête en vertu de la LPRPDE n^{o} 2005-319, Commissariat à la protection de la vie privée du Canada (CPVP), 8 novembre 2005

Fausse adresse source

Se reporter aux rapports suivants :

- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, Paul Ferguson et Daniel Senie, The Internet Society, mai 2000 (RFC 2827) [en anglais seulement]

- Ingress Filtering for Multihomed Networks, RFC 3704, Fred Baker et Pekka Savola, The Internet Society, mars 2004 (mise à jour de la RFC 2827) [en anglais seulement]

- RFC 3013

- Pratiques exemplaires de sécurité pour les fournisseurs de services de télécommunications canadiens (FST) [article 3.1.4, contrôle 2], Comité consultatif canadien pour la sécurité des télécommunications (CCCST), 31 octobre 2013

Blocage du trafic Internet en fonction des signatures de fichiers

Cette méthode repose sur la reconnaissance de modèles connus de distribution et d'exécution de logiciels malveillants ou d'autres comportements qui caractérisent les infections du système ou les méthodes d'attaque connues. Le trafic en temps réel est comparé à un référentiel de signatures et bloqué en cas de correspondance.

La Norme de surveillance de la sécurité du réseau et de détection des risques pour les fournisseurs canadiens de services de télécommunications (FCST), Groupe de travail sur la protection cybernétique des télécommunications canadiennes pour le CCCST, 20 janvier 2020 énonce que les FST doivent être en mesure de détecter par signature les logiciels malveillants opérant dans leurs réseaux. De plus, les réponses aux demandes de renseignements du Conseil montrent que Rogers Communications Canada Inc., Shaw Communications Inc., TekSavvy Solutions Inc. et Xplornet Communications Inc. utilisent chacune une certaine forme de blocage par signature dans le cadre de leurs stratégies de blocage respectives.

Blocage de renseignements en fonction des empreintes digitales du réseau

Un regroupement de renseignements basé sur l'échange qui se produit entre deux appareils au moment de l'initiation d'une connexion sur Internet (c.-à-d. basé sur l'information échangée dans une prise de contact à trois voies TCP [protocole de contrôle de transmission]). Les éléments de cet échange qui peuvent catégoriser l'objectif d'un appareil, même un appareil malveillant, comprennent le nombre de fois qu'un appareil tente de retransmettre ou le laps de temps entre les retransmissions. Lorsqu'ils sont suffisamment uniques, ces éléments peuvent être utilisés pour prendre les empreintes digitales des serveurs de commande et de contrôle et d'autres appareils malveillants.

Inspection approfondie des paquets

L'inspection approfondie des paquets (IAP) est une forme de filtrage de paquets de réseau informatique qui existe depuis plusieurs années. Lorsqu'elle est utilisée aux fins de cybersécurité, l'IAP peut permettre d'examiner les données ou l'en-tête d'un paquet lorsqu'il passe par un point d'inspection, à la recherche d'indications de non-respect du protocole, de logiciels malveillants et d'autres formes d'intrusion.

Les technologies de l'IAP soulèvent des préoccupations en matière de protection de la vie privée parce qu'elles peuvent comprendre l'inspection de renseignements transmis par Internet, comme l'indiquent la soumission et les répliques finales du CPVP au Conseil dans le cadre de l'instance concernant les pratiques de gestion du trafic Internet ayant mené à l'*Examen des pratiques de gestion du trafic Internet des fournisseurs de services Internet*, Politique réglementaire de télécom CRTC 2009-657, 21 octobre 2009.

Open Xchange et Vaxination Informatique ont initialement déconseillé l'autorisation de l'IAP, tandis que TELUS Communications Inc. a mentionné dans sa contribution [en anglais seulement] au Comité directeur du CRTC sur l'interconnexion que le blocage des réseaux de zombies à d'autres niveaux, comme l'IAP, est utile et devrait être encouragé, ce qui laisse supposer qu'il est déjà utilisé.

Dans le rapport La commissaire adjointe recommande à Bell Canada d'informer les clients au sujet de l'inspection approfondie des paquets, Rapport de conclusions en vertu de la LPRPDE nº 2009-010, septembre 2009, le CPVP a recommandé que Bell Canada informe ses clients au sujet de l'IAP qu'elle effectuait. Toutefois, il n'est pas clair si cette recommandation a été mise en œuvre par Bell Canada et d'autres entreprises utilisant la même technologie.