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

Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9

PDF version

Ottawa, 13 January 2021

Public record: 1011-NOC2021-0009

Call for comments – Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety

Deadline for submission of interventions: 15 March 2021

[Submit an intervention or view related documents]

The Commission hereby calls for comments on its proposal to develop a network-level blocking framework that will limit the harm botnets cause to Canadians while safeguarding privacy and ensuring transparency. Botnets are the basis for an increasingly large proportion of cyber threats to Canadian citizens, corporations, and institutions, and blocking botnet traffic is an effective way to reduce those threats.

Background

1. Malicious cyber activity targets Canadian consumers and businesses, as well as organizations that provide critical services such as hospitals, schools, and government bodies. This malicious activity compromises privacy and impairs network integrity and availability. It also imposes costs on the victims and undermines Canadians' confidence in the use of electronic communications to carry out their online activities.

2. A trend in cyber attacks is the use of botnets to subvert defenses and give attackers an added layer of anonymity. A botnet is a network of malware-infected computers (bots) that are under the control of a command and control (C2) server operated by a malicious actor. The malware infection is caused by a computer program installed without the computer owner's knowledge or consent. Each bot[1] is an Internet subscriber's computer or other device that communicates through the subscriber's service provider en route to an associated C2 server.

3. Botnets underpin an increasingly large proportion of malware and facilitate the most egregious forms of cyber threats. The types of cyber attack enabled by botnets include spam distribution, distributed denial-of-service attacks, information theft, and malware deployment. Of particular concern to Canadians are frequent

[1] The bots referred to in this Notice of Consultation are exclusively malware-infected devices. "Good" bots programmed to perform helpful tasks, such as chatbots and crawler bots, are excluded from consideration.

ransomware[2] attacks, which have caused significant service disruptions and financial damage.

4. The Commission regulates the Canadian telecommunications system with a view to furthering the Canadian telecommunications policy objectives set out in section 7 of the *Telecommunications Act* (the Act). Malicious activity facilitated by botnets is contrary to several of the Act's policy objectives, including

    - facilitating the development of a telecommunications system that serves to safeguard, enrich, and strengthen the social and economic fabric of Canada and its regions;
    - rendering reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada;
    - responding to the economic and social requirements of users of telecommunications services; and
    - contributing to the protection of the privacy of persons.

5. The Commission is also the principal enforcement agency for *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activity, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act* (Canada's Anti-Spam Legislation [CASL]). It is responsible for ensuring compliance with provisions relating to spam distribution (section 6), malicious network traffic redirection (section 7), and malware installation (section 8), as well as for enforcing the prohibition on aiding anyone engaging in those activities (section 9). Commission staff conducts investigations and takes enforcement measures where violations have already occurred, and also works proactively to prevent violations using compliance promotion and outreach mechanisms. Botnet activity is by definition a CASL violation, as is the botnet itself.

6. In Compliance and Enforcement Information Bulletin 2018-415 the Commission noted that section 9 of CASL may apply to individuals and organizations, including Canadian carriers and other telecommunications service providers (TSPs), who provide technical and other enabling services that facilitate electronic commercial activity. The Commission stated that, pursuant to section 9, it expected TSPs to take appropriate steps to reduce and limit anti-CASL behaviour on their networks.

[2] Ransomware is a type of malicious software designed to deny access to a computer system or data by encrypting it until a ransom is paid. The most common method of ransomware distribution is phishing spam, where a victim opens an email containing a malicious attachment and unknowingly downloads it onto their computer.

7. One way that TSPs can limit anti-CASL behaviour is by blocking botnet traffic. Some blocking mechanisms can be implemented at endpoints by users, and others at the network level by service providers, including Canadian carriers and other TSPs. However, section 36 of the Act also contains a prohibition on the control of content of telecommunications by Canadian carriers.

8. The Commission usually cannot tackle botnet-facilitated attacks at their source, since these are most often outside of Canada. However, the Commission does have the authority and mandate to use the regulatory mechanisms in the Act to address malicious activity facilitated by botnets. The Commission is therefore considering the development of a network-level blocking framework to prevent harm and achieve the objectives of the Act.

Network-level blocking framework

9. Service providers can introduce network-level blocking using a variety of techniques. Three of the most common are domain-based blocking, Internet Protocol (IP)-based blocking, and protocol-based blocking.

10. Internet users access websites by clicking on links or by entering domains (www.example.com) into a browser. To access a webpage, the domain has to first be translated into the IP address of the server that hosts the webpage. This translation happens through the Domain Name System (DNS), which maps domain names to IP addresses. Once the IP address is found, the Internet user's device can then route communication to the website's server and download the webpage.

11. When domain-based blocking is in place and an infected device requests a blocklisted C2 domain, the response from the DNS will either reply that the domain is unknown or will redirect the user to a site stating that the requested domain is not permitted.

12. However, not all malware connects to C2 servers using domains – some connect by communicating directly with a C2 server's IP address. Domain-based blocking is not effective for this type of malware because it bypasses the DNS, so alternative techniques are required. One alternative is IP-based blocking, which uses a filter called a firewall to prevent communication to the IP addresses of suspected C2 servers while letting other communication through. Another is protocol-based blocking, which is a more targeted form of IP-based blocking limited to a select group of services on a specified server.

13. All of these blocking techniques use intelligence from public and private sources to identify and block access to C2 servers via their domain names, IP addresses, or known botnet communication patterns.

14. The Commission's preliminary view is that network-level blocking is a viable strategy to prevent the harm botnets cause to Canadians and to promote the Act's policy objectives.

15. While network-level blocking can be implemented without accessing the content of Internet transmissions, the Commission nevertheless considers that any regulatory framework for blocking or filtering traffic must include safeguards to ensure user interests are protected. Any framework the Commission approves will need to include, at a minimum, provisions that (i) ensure Internet subscriber privacy, (ii) enable subscribers to opt into or out of blocking, (iii) provide a false-positive correction mechanism, (iv) ensure blocking decisions are unbiased and made in the best interest of Canadians, and (v) minimize subscriber information monitoring, collection, and usage.

Call for comments

16. In order to better safeguard Canadians from malicious communications and to increase cyber safety, the Commission is committed to efforts that prevent, reduce, and disrupt botnets and other anti-CASL communications.

17. The Commission hereby initiates a call for comments to guide development of a network-level blocking framework to limit the harm caused to Canadians by botnets. The Commission seeks input from Internet service subscribers on the first question below, and from all stakeholders on the remaining matters.

Q1. As a Canadian Internet user, how would you benefit from having your TSP block malicious botnet communications? What concerns do you have?

18. Net neutrality is the concept that all Internet traffic should be given equal treatment by TSPs with little or no prioritization, discrimination, or preference, regardless of the content of the traffic. The Commission has endorsed this concept in principle, though it supports limited exceptions, for example to programs that block access to child exploitation material, and to services such as TSP spam filters.

19. Traffic from botnets exposes Canadians to spam, spyware, information theft, and ransomware. Given the risks associated with this exposure, a limited exception to net neutrality may be warranted in order to offer Canadians additional protections from these threats.

20. The Commission seeks input from Canadian Internet service subscribers on whether they believe they could benefit from a framework that allows their TSP to block botnet traffic, and their reasons for this opinion.

Q2. What framework conditions are required to safeguard Internet service subscribers' privacy during traffic monitoring and blocking program reporting?

21. Botnets pose a significant threat to consumer privacy. They are used to gain unlawful access to sensitive personal information that can then be used for malicious ends. Blocking botnet communications can help protect consumers; however, this protection is achieved by monitoring Internet traffic. The consequences for consumer privacy that monitoring causes must be addressed by any potential blocking framework.

22. The Commission invites parties to comment on conditions that can protect consumer privacy, such as

    - prohibiting carriers from monitoring, collecting, or disclosing content or metadata that does not contribute to blocking botnet traffic;
    - limiting monitoring and collection to the destination domain name or IP address requested and the number of times the malicious service is requested; and
    - restricting disclosure of monitored data to parties participating in the blocking program.

23. The Commission also seeks comments on the appropriate metrics to use to ensure the framework is functioning as intended. Examples include the timestamps and volumes of blocking events and the false-positive rate.

Q3. What are the necessary disclosure requirements for carriers and TSPs to ensure Internet subscribers have sufficient information to make informed decisions about participating in a blocking program?

24. Blocking program transparency is important to ensure accountability and to help consumers make informed choices when selecting their TSP or deciding whether to participate in a blocking program. Internet service subscribers should be informed by their TSP that blocking is being employed, and should be able to check whether a particular domain or IP address is blocked by their provider. However, to ensure that a blocking program remains effective, it may be reasonable to put limits on what information is made available, since malicious actors could use any public information to circumvent the blocking measures.

25. The Commission invites comments on provisions that will provide transparency about blocking programs, for example notifying customers of the scope of filtering mechanism or creating a subscriber portal to check whether a particular domain is being blocked. In their comments parties should address any risks to efficiency or success associated with disclosing information about how the program operates.

Q4. Which parties are best suited to decide what is blocked?

26. Decisions to block should not be made lightly, and need to take into account factors such as the level of potential harm to Internet users and whether the blocking will have other unintended effects. Blocking decisions must be free of commercial interests and be based on robust data from trusted sources. The Commission's preliminary view is that an independent party with expertise in cyber security would be best suited to assess the impact of blocking a particular domain or IP address with a view to protecting public interest, and to decide whether blocking is warranted.

27. The Commission is also of the view that while carriers and TSPs may require flexibility to remove from the blocklist indicators that lead to false positives, to protect the integrity of the framework they would need to seek approval from the independent assessor before adding new indicators.

28. The Commission invites parties to comment on methods and provisions to ensure unbiased and accurate blocking decisions, and to identify viable, independent parties that may be able to serve as the decision-making authority.

Q5. Would botnet traffic be best addressed by default blocking with an option to opt out, or by a model that allows opt-in blocking?

29. Infected Internet-connected devices operating as bots generally do so without the owner's knowledge or consent. Internet service subscribers may not see the benefit of participating in a network-level blocking program, even if their device is infected with malware, which may make an opt-in model less effective than an opt-out one.

30. The Commission invites parties to compare and contrast the effectiveness of block-by-default models versus opt-in models to address botnet communications. Parties should identify their preferred model and provisions required for its implementation.

Q6. What framework provisions or conditions are required to prevent and mitigate the risks associated with over-blocking and false positives?

31. Multiple online services can resolve to the same IP address, and botnet C2 servers do not usually remain on the same device for extended periods of time. Blocking an IP address may therefore inadvertently prevent access to a legitimate service, and blocking a C2 server will be effective for only a limited time. Consequently, the blocklist must change regularly to remain accurate, which introduces risks of over-blocking and false positives.

32. The Commission invites comments on blocking framework provisions or conditions that could prevent over-blocking and false positives, or could mitigate the associated risks. Parties are asked to

    - comment on the likelihood and impact of over-blocking and false positives in the context of safeguards against botnet traffic;
    - set out expectations for resolving false positives and provisions to ensure timeliness and procedural fairness in the resolution process; and
    - suggest options for automated means to resolve incorrectly blocked services, and their associated benefits and drawbacks.

Q7. What regulatory mechanism is best suited to ensure implementation of a network-level blocking framework that effectively addresses botnet communications?

33. The Commission considers that it has a number of powers under the Act that would allow it to establish either a mandatory or voluntary framework, including those in sections 24, 24.1, 36, and 41. For example, the Commission might consider

- authorizing Canadian carriers to block under the authority of section 36 of the Act;
- imposing a requirement on Canadian carriers and other TSPs to perform network-level blocking as a condition of service, pursuant to sections 24 and 24.1;
- prohibiting the use of a Canadian carrier's telecommunications facilities to transmit botnet communications, insofar as these are unsolicited communications under section 41 of the Act.

34. The Commission could also consider using section 42 of the Act to extend this framework to other persons who have control over telecommunications facilities.

35. The Commission invites feedback on the appropriateness and effectiveness of the regulatory mechanisms above to address the harm caused by botnets. Parties are encouraged to consider all of the options listed and provide comments on each.

Q8. Which network-level blocking techniques are best suited to stop or limit botnet communication?

36. Botnets and the malware they rely on vary by design and purpose. These variations may limit the effectiveness of certain blocking techniques against botnet traffic.

37. The Commission seeks comments on the effectiveness of botnet blocking techniques, particularly those that block communications from an infected device in Canada to C2 servers within or outside Canada.

38. In light of the significant increase in botnet-facilitated attacks, the Commission will focus on techniques that balance effectiveness and ease of implementation, and that avoid additional costs to Internet service subscribers. Techniques that leverage existing technologies, services, and infrastructure are therefore of particular interest.

39. Parties are requested to identify their preferred blocking techniques and provide a detailed supporting rationale that outlines their benefits, drawbacks, costs, implementation speed, and implementation barriers. As part of their description of drawbacks, parties are asked to comment specifically on gaps in network defences that would remain in spite of implementation, false-positive rates, and over-blocking risks.

40. Comments need not be limited to domain-, IP-, or protocol-based methods. Parties are encouraged to propose alternatives and identify all associated benefits and drawbacks.

Q9. If domain-based blocking is identified as a preferred technique, which domain resolver selection considerations would a blocking framework need to take into account?

41. Domain resolvers are specialized computers managed by service providers that start the process of translating a domain name into its corresponding IP address. Many domain resolvers and services are available to provide domain blocking and prevent access to botnet C2 servers.

42. The Commission invites comments on the potential use of existing domain resolvers or services to block botnet traffic, including CIRA Canadian Shield, Quad9, OpenDNS, Comodo Secure DNS, and CleanBrowsing.

43. Parties should address considerations with respect to use of existing domain resolvers adapted to botnet communications. Parties may also propose the use of particular domain resolvers with a rationale identifying their benefits and drawbacks.

Q10. How should technology changes be addressed in the network-level blocking framework?

44. Botnets are dynamic and flexible by design. Botnet malware is frequently modified and updated to replenish or expand the bot pool, add functionality, and increase performance. C2 servers are also regularly moved and duplicated to different servers to evade detection and resist takedowns. The large number of botnets in operation engage in a variety of communication behaviours that are increasingly encrypted and therefore difficult to detect. Operators adapt botnet design to bypass any known blocking methods; an effective blocking framework must be able to adapt in kind.

45. The Commission invites suggestions and comments on framework provisions that would assist carriers and other TSPs to adjust to variations in botnet design and to adaptations by operators. For example, what provisions should the framework include to account for changes in malware design or types of devices targeted by botnet operators?

Procedure

46. The *Canadian Radio-television and Telecommunications Commission Rules of Practice and Procedure* (the Rules of Procedure) apply to this proceeding. The Rules of Procedure set out, among other things, the rules for the content, format, filing, and service of interventions, answers, replies, and requests for information; the procedure for filing confidential information and requesting its disclosure; and the conduct of public hearings. Accordingly, the procedure set out below must be read in conjunction with the Rules of Procedure and related documents, which can be found on the Commission's website at www.crtc.gc.ca, under "Statutes and regulations." The guidelines set out in Broadcasting and Telecom Information Bulletin 2010-959 provide information to help interested persons and parties understand the Rules of Procedure so that they can more effectively participate in Commission proceedings.[3]

[3] Sections 30 to 34 of the Rules of Procedure and sections 38 to 39 of the Act set out a process by which parties to Commission proceedings may file information on the record of a public proceeding in confidence. Consult Broadcasting and Telecom Information Bulletin 2010-961 for details about the process.

47. The Commission encourages responses from, among others, incumbent and competitive local exchange carriers, web hosting companies, protective DNS providers, and other governmental organizations whose mandates include safeguarding critical infrastructure or computer networks.

48. Interested persons who wish to become parties to this proceeding must file an intervention with the Commission regarding the above-noted issues by **15 March 2021**. The intervention must be filed in accordance with section 26 of the Rules of Procedure.

49. Parties are permitted to coordinate, organize, and file, in a single submission, interventions by other interested persons who share their position. Information on how to file this type of submission, known as a joint supporting intervention, as well as a template for the accompanying cover letter to be filed by parties, can be found in Telecom Information Bulletin 2011-693.

50. All documents required to be served on parties to the proceeding must be served using the contact information contained in the interventions.

51. All parties may file replies to interventions with the Commission by **14 April 2021**. Submissions, including an executive summary, are not to exceed 20 pages.

52. The Commission encourages interested persons and parties to monitor the record of this proceeding, available on the Commission's website at www.crtc.gc.ca, for additional information that they may find useful when preparing their submissions.

53. Submissions longer than five pages should include a summary. Each paragraph of all submissions should be numbered, and the line ***End of document*** should follow the last paragraph. This will help the Commission verify that the document has not been damaged during electronic transmission.

54. Pursuant to Broadcasting and Telecom Information Bulletin 2015-242, the Commission expects incorporated entities and associations, and encourages all Canadians, to file submissions for Commission proceedings in accessible formats (for example, text-based file formats that enable text to be enlarged or modified, or read by screen readers). To provide assistance in this regard, the Commission has posted on its website guidelines for preparing documents in accessible formats.

55. Submissions must be filed by sending them to the Secretary General of the Commission using **only one** of the following means:

by completing the
[Intervention form]

or

by mail to
CRTC, Ottawa, Ontario K1A 0N2

or

by fax to
819-994-0218

56. Parties who send documents electronically must ensure that they will be able to prove, upon Commission request, that filing, or where required, service of a particular document was completed. Accordingly, parties must keep proof of the sending and receipt of each document for 180 days after the date on which the document is filed or served. The Commission advises parties who file or serve documents by electronic means to exercise caution when using email for the service of documents, as it may be difficult to establish that service has occurred.

57. In accordance with the Rules of Procedure, a document must be received by the Commission and all relevant parties by 5 p.m. Vancouver time (8 p.m. Ottawa time) on the date it is due. Parties are responsible for ensuring the timely delivery of their submissions and will not be notified if their submissions are received after the deadline. Late submissions, including those due to postal delays, will not be considered by the Commission and will not be made part of the public record.

58. The Commission will not formally acknowledge submissions. It will, however, fully consider all submissions, which will form part of the public record of the proceeding, provided that the procedure for filing set out above has been followed.

Important notice

59. All information that parties provide as part of this public process, except information designated confidential, whether sent by postal mail, fax, email, or through the Commission's website at www.crtc.gc.ca, becomes part of a publicly accessible file and will be posted on the Commission's website. This includes all personal information, such as full names, email addresses, postal/street addresses, and telephone and fax numbers.

60. The personal information that parties provide will be used and may be disclosed for the purpose for which the information was obtained or compiled by the Commission, or for a use consistent with that purpose.

61. Documents received electronically or otherwise will be posted on the Commission's website in their entirety exactly as received, including any personal information contained therein, in the official language and format in which they are received. Documents not received electronically will be available in PDF format.

62. The information that parties provide to the Commission as part of this public process is entered into an unsearchable database dedicated to this specific public process. This database is accessible only from the web page of this particular public process. As a result, a general search of the Commission's website with the help of either its search engine or a third-party search engine will not provide access to the information that was provided as part of this public process.

Availability of documents

63. Electronic versions of the interventions and other documents referred to in this notice are available on the Commission's website at www.crtc.gc.ca by using the public record number provided at the beginning of this notice or by visiting the "Consultations and hearings – Have your say!" section, then selecting "our applications and processes that are open for comment." Documents can then be accessed by clicking on the links in the "Subject" and "Related Documents" columns associated with this particular notice.

64. Documents are also available at the following address, upon request, during normal business hours.

    Les Terrasses de la Chaudière
    Central Building
    1 Promenade du Portage
    Gatineau, Québec
    J8X 4B1
    Tel.: 819-997-2429
    Fax: 819-994-0218

    Toll-free telephone: 1-877-249-2782
    Toll-free TTY: 1-877-909-2782

Secretary General

Related documents

- *Guidelines on the Commission's approach to section 9 of Canada's anti-spam legislation (CASL)*, Compliance and Enforcement Information Bulletin CRTC 2018-415, 5 November 2018

- *Filing submissions for Commission proceedings in accessible formats*, Broadcasting and Telecom Information Bulletin CRTC 2015-242, 8 June 2015

- *Filing of joint supporting interventions*, Telecom Information Bulletin CRTC 2011-693, 8 November 2011

- *Procedures for filing confidential information and requesting its disclosure in Commission proceedings*, Broadcasting and Telecom Information Bulletin CRTC 2010-961, 23 December 2010; as amended by Broadcasting and Telecom Information Bulletin CRTC 2010-961-1, 26 October 2012

- *Guidelines on the CRTC Rules of Practice and Procedure*, Broadcasting and Telecom Information Bulletin CRTC 2010-959, 23 December 2010