From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

To: Canadian Radio-television and Telecommunications Commission (CRTC)

Date: March 15th, 2021

Re: "Call for comments – Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians 'online safety", Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9, Public record: 1011-NOC2021-0009, as published online at https://crtc.gc.ca/eng/archive/2021/2021-9.htm.

Dear Commissioners:

Thank you for your interest in combating botnets and malicious software, and for the opportunity to offer input to this proceeding. M3AAWG appreciates the invitation to comment on this proceeding. Paragraph 17 of the call for comments stated: "The Commission seeks input from Internet service subscribers on the first question below, and from all stakeholders on the remaining matters."

Since Question 1 was addressed to "Canadian Internet user(s)," we'll refrain from addressing that question, but offer feedback on many other questions posed by the CRTC. We've generally organized our response according to the order questions were posed by the CRTC, referenced our comments to the Call for Comments paragraph numbers and categorized most comments as a consideration or recommendation.

Our detailed comments run approximately ten pages, we have included a brief summation pursuant to Paragraph 53 of the Call for Comments, which mandates that "Submissions longer than five pages should include a summary."

Summation

Consideration: Botnets are a global problem, and tackling the botnet problem will require a collaborative multinational approach. The CRTC and the Government of Canada are well-positioned to lead that work (if willing to voluntarily undertake a burden of this magnitude).

Consideration: Service providers, both in Canada and abroad, already play a critical role in combating not only botnets, but in protecting subscribers and critical network resources from other cyberthreats. Their continued ability to do so requires that they have the option, but not the obligation, to implement appropriate data-driven measures against harmful and/or unwanted traffic. The ability of service providers to continue to successfully combat network abuse requires the ability to collaborate on cybersecurity-related matters. It will also require some tolerance for unintentional privacy violations by well-intentioned defenders, and protection from lawsuits aimed at derailing and inhibiting work on botnet monitoring and countermeasures.

Recommendation: M3AAWG would urge CRTC to adopt a privacy framework broad enough to encompass support for the much-needed anti-spam, anti-phishing, scam defense and anti-malware efforts. Furthermore, some safe harbor provisions must be included in the framework to ensure that service providers feel safe in providing security.

Consideration: While the Call for Comments framed the potential technical blocking work in the context of brute force techniques such as blocking domain names or IP addresses, our comments highlighted the need for a potentially more flexible and nuanced approach. For example, some sites might have many legitimate pages plus perhaps a single malicious download. Blocking such a site by IP address alone (or domain name alone) might result in substantial collateral damage. Providers must be free to employ a panoply of currently known and still-to-be-developed methods in combating botnets.

Consideration: The Call for Comments discussed potentially allowing users to obtain granular information on service provider protective measures. We explained that this may be highly technical information that may be of little use to average users, and other problems with that approach, including both tactical issues (attackers will leverage this information to avoid specific defensive measures), and strategic problems (some highly effective approaches only remain effective because attackers aren't aware of the approaches being used). We recommend that, where practical without great cost or complexity, individuals be given the flexibility to opt-out of service provider filtering and blocking should they desire to do so, but not the authority to demand details or location of blocking and filtering.

Consideration: The Call for Comments also potentially envisioned an industry-wide, centrally-administered response. We recommend giving providers the flexibility to collaborate, but not the mandate to employ a single one-size-is-supposed-to-fit-all centralized "solution" to botnet-related challenges. Allowing a diversity of approaches avoids the risks of monoculturalism, and will incentivize continued innovation and progress in technical approaches to tackling botnets.

Consideration: M3AAWG concurs that ensuring user privacy is important. It is our belief that the privacy of Canadian Internet users can be increased through use of strong encryption, but that this comes at a cost of reduced protection; many forms of abuse only become apparent when content is visible. In cases (e.g., banking) where strong content and/or metadata privacy are required, the existing internet practices of using end-to-end encryption and/or anonymizing VPNs such as TOR may be a more appropriate solution for Canadians than precluding content and metadata based defenses in the pursuit of maximum privacy at all cost.

Consideration: M3AAWG appreciates the opportunity to share the above major points, urges the Commission to see our more detailed response for additional commentary, and stands ready to address any follow-up questions you may have.

Detailed Comments

Regarding Call for Comments Question 2, "*What framework conditions are required to safeguard Internet service subscribers 'privacy during traffic monitoring and blocking program reporting?*" The Commission suggests in Call for Comments paragraph 22 that this might be accomplished via regulatory mechanisms, 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."*

M3AAWG urges the CRTC to reconsider the above potential restrictions based on the following:

Recommendation: Network service providers should always be permitted (but not required) to monitor, collect and share network traffic and device telemetry as may be necessary for legitimate purposes such as:

- Operation & protection of the service provider's assets (including its networks, systems, software, and data),
- Routine delivery of contracted or requested services and products to customers and partners,
- Network modeling, capacity planning, and traffic engineering,
- Usage tracking, charging, and billing,
- Problem identification and diagnosis, fault resolution, and preventive maintenance,
- Blocking, diverting, or otherwise managing unwanted or illegal traffic,
- Compliance with applicable court orders, subpoenas and other compulsory demands for information.

Recommendation: Limiting monitoring and collection to the destination domain name or IP address requested and the number of times the malicious service is requested should not be imposed as it would be disastrous from a cybersecurity perspective for the following rationale:

- Any single host may offer diverse services on different ports. For example, a host might have ssh on port 22, SMTP on port 25, HTTP on port 80, HTTPS on port 443, etc. Botnets often co-exist among those well-known services on high number ephemeral ports (or other ports of the bot controller's choice). If the carrier were to be prevented from collecting **destination port information,** it would be impossible for the carrier to differentiate between legitimate services and unauthorized services running on the same destination host.
- Many service providers voluntarily work to identify and notify malware-infested customers. Doing so requires the ability to identify *which customer* is reaching out to known botted hosts. Performing that analysis typically requires **source IP address, source port information, and an accurate time stamp (with time zone).** If a carrier was prevented from acquiring or exploiting that information, many malware-infested customers will end up remaining unmitigated and persistently abused or open for abuse, directly contrary to the Commission's apparent interest in combating bots.
- Public safety authorities need Internet service providers and mobile carriers who have implemented Carrier Grade Network Address Translation (Carrier Grade NAT or CGN) in which, very simply put, they create large local area networks assigning one single public IP address to a number of their customers, as opposed to assigning one public IP address per customer, to be able to identify port information and accurate time stamps for their customers ' traffic. Protocol information and time stamps are technically needed in any CGN implementation to identify the origin of traffic that may be malicious or harmful in nature. Without these data, service providers and public safety authorities may be hard pressed to identify the source of any given activity.
- Identifying malicious payloads (or online Child Sexual Abuse Materials for that matter) is often done using **cryptographic hashes** that act as a unique signature for executables, images or other

files. As written, the proposed limitation would preclude carriers from leveraging hash-based approaches.

Recommendation: To effectively mitigate attacks, the cyber defense community must be allowed to collaborate and share intelligence and therefore requires provisions to allow for disclosure of monitored data to parties participating outside of the blocking program. Safe browsing mechanisms, malware removal and anti-phishing takedown services are poignant examples of the need for community sharing of URIs, malicious application identity and potentially infected device identity.

Consideration: While the Call for Comments focused on consumer privacy in terms of CRTC expectations for service providers, the inquiry also explicitly suggests a role for third parties, to at least potentially include third party DNS providers (see Call for Comments at Paragraph 41-43). Given the potential privacy sensitivity of below-the-recursor DNS queries, we urge the CRTC to expand any privacy review to go beyond just broadband service providers to also encompass any third parties who may be offering network security services via DNS or other protocols.

Consideration: Regarding Call for Comments paragraph 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."* , false negative rates are equally important to determine failures to block unsafe content and therefore should be added as a metric.

Regarding Call for Comments paragraph 24, *"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.",* M3AAWG urges the CRTC to contemplate the following:

Consideration: While the described model envisions a tool which can accept a domain or IP and report whether that domain or IP is "blocked" or "unblocked" is an extremely simplistic blocking model. Many techniques used to manage dangerous or unwanted traffic may be far more subtle or contextual. For example, a legitimate site that has both legitimate pages (that SHOULD NOT be blocked), and a single malicious executable (that SHOULD be blocked).

Consideration: Combating unwanted traffic can potentially be very costly requiring specially trained staff, significant data storage and computational resources - taking years to develop and refine proprietary techniques and methods.

Consideration: To further CRTC's recognition of the possible need to publicly limit information on blocking measures - highly effective sources and methods for managing unwanted traffic may be rendered completely ineffective if publicly disclosed. Even the ability of malicious actors to simply probe the blocking status for domains and IPs may circumvent the blocking measures.

Consideration: End users who may want to do so are able to bypass most service provider filtering by simply using a virtual private network (VPN). Under those circumstances, an end user may circumvent a service provider's default filtering *without* needing to learn specifics about the service provider's default filtering.

Consideration: End users may not have the background and experience needed to correctly interpret filtering and blocking rules, even if they were to be fully disclosed to them.

Regarding Call for Comments paragraph 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."*, M3AAWG urges the CRTC to contemplate the following:

Consideration: Call for Comments paragraph 26 does not appear to acknowledge that many service providers may *already* routinely block dangerous sites and malicious or unwanted traffic, or both. The surgical precision and professional care applied to this work is discernible most readily in the fact that many people may not even know that this filtering is taking place -- collateral damage is typically held to a virtually nil level.

Consideration: Regarding "*Blocking decisions must be [...] based on robust data from trusted sources.",* often blocking decisions will be based on locally-collected data. Internet service providers and mobile carriers assume that such data would be considered to be "robust" and "from a trusted source" by default. When it comes to data from third-party sources, like DNS blocklists, data is typically offered on a "take-it-or-leave-it" basis. Internet service providers and mobile carriers should define and implement criteria for the selection of the domain blocklist providers they use. An example has been defined by ICANN within the methodology of its Domain Abuse Activity Reporting system (DAAR) (https://www.icann.org/en/system/files/files/daar-methodology-paper-30nov17-en.pdf), particularly beginning on page 14 (Selection of Reputation).

Recommendation: Regarding "*... 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."*, we urge the continuation of a decentralized provider-by-provider filtering regime over the adoption of a single independent party to make industry-wide blocking or filtering decisions.

Consideration: A diversity of filtering approaches is important for system resilience and robustness. Employing a diversity of approaches confuses attackers and compensates for vulnerabilities within any one given technology or implementation. Additionally, divers filtering approaches support and encourage innovation.

Consideration: Regarding Call for Comments Paragraph 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."*, sophisticated attack sources operate and can be identified at rates of 500 new indicators per minute. A single "independent assessor" providing industry-wide services could easily be overwhelmed when attempting to review and approve a stream of such discoveries at full line rate with minimal delay. The industry needs filtering implementations that work at industrial scale, not *ad hoc* approaches that will fail to scale.

Consideration: Regarding Call for Comments Paragraph 29, this paragraph asks, *"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."*, M3AAWG agrees an opt-in model may see poor uptake. Our belief is that the correct model is one that protects most users by default. We also recognize that users will always be able to evade protective measures if sufficiently motivated to do so. For example firewall rules could be circumvented through the use of a virtual private network, or DNS-

based filtering (such as RPZ, https://dnsrpz.info/) by using a 3rd-party DNS provider (perhaps via DNS over HTTPS [DoH] or DNS over TLS [DoT]).

Consideration: Regarding Call for Comments Paragraph 32, "*comment on the likelihood and impact of over-blocking and false positives in the context of safeguards against botnet traffic*", M3AAWG believes the potential for over-blocking is high if blocking is only done via domain names and IP addresses (as previously explained above). Malicious content may co-exist with legitimate content on the same domain name or IP address, or only be delivered if or when suitable preceding conditions may exist (such as an appropriate referrer agent value or user agent string when visiting a web site).

Consideration: Regarding Call for Comments Paragraph 32, "*set out expectations for resolving false positives and provisions to ensure timeliness and procedural fairness in the resolution process*", the first factor that must be considered is the role of the person seeking to remove a block:

- Is it a technically-knowledgeable representative of a service provider, seeking to resolve an urgent problem such as the inadvertent blocking of a major site?
- Or is it an end-user, inconvenienced by being unable to visit an obscure (and unquestionably malware-infected) site?
- Or is it a bot controller or a malware author seeking to neutralize a network block interfering with the malware they've developed or deployed, or both?

Consideration: For the purposes of this response, we do not consider the case where a site is properly listed ("true positives"), but note that a request to handle a false positive issued by a technically knowledgeable and trusted carrier representative must be handled with dispatch, typically in at most a matter of hours.

Consideration: Regarding Call for Comments Paragraph 32, "*suggest options for **automated** means to resolve incorrectly blocked services, and their associated benefits and drawbacks*"[emphasis added], consider delisting requests made to anti-spam block list providers. Most delisting requests require manual processing by block list provider staff, a potentially time-consuming process that can require substantial expertise. Delisting of botnet blocks will likely be similar. A noteworthy exception is largely-automated processes used by a couple of anti-abuse parties like the CBL (the Composite Blocklist, see https://www.abuseat.org/, The Spamhaus Project https://www.spamhaus.org/). Because these automatically detect and list compromised hosts, it allows users to correct the problem that results in the listing, and then request delisting via a web form. The IP will then normally get delisted. However, if the problem has not been corrected, the block will typically simply get automatically reinstated. If automatic detection processes drive the listing process, this might be a noteworthy approach to consider.

Consideration: Regarding Call for Comments Paragraph 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."*, botnets frequently include capabilities like domain generation algorithms ("DGAs") to ensure that even if a botnet's customary control channel gets blocked, a new backup channel can be established and used as a fallback to regain control. Specifically, DGAs typically use a non-public algorithm to nominate some number of alternative C&C domains as fallback domains every day. As long as ONE of those alternative C&C hosts can be registered and used by the bot controller, the bots can check in and the bot controller can retain control of his or her bots. To successfully block access to that bot, all the domains generated by the DGA must be denied to the bot controllers. This can be achieved via different ways:

- A defender paying for the registration of all those domains (but their numbers can easily reach thousands potentially being cost prohibitive).,

- Preventing those domains from being registered at the Top-Level Domain (which is sometimes not feasible, particularly if the DGA is creating domains under country code Top-Level Domains),

- Allowing those domains to be registered but suspending them at the point of creation by setting their status in a serverHold,

- Adding nameservers for those domains that are controlled by law enforcement or security researchers, as appropriate.

Consideration: Botnet authors might also elect to use a non-DNS-based decentralized naming system (such as a peer-to-peer naming system). For example, consider https://handshake.org/ or dot onion addresses from Tor. To the extent that these mechanisms totally bypass the domain name system, attempting to block access to those alternatives via the DNS would be ineffective.

Consideration: Botnet authors might also elect to encrypt or tunnel their C&C traffic. Simplistic solutions will not be adequate to detect and interdict opaque C&C traffic of that sort.

Consideration: Call for Comments Paragraph 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 defenses that would remain in spite of implementation, false-positive rates, and over-blocking risks."*, M3AAWG does not have a recommendation on any preferred blocking technique, and encourages the use of multiple techniques. To promote the goal of keeping Canadian computers (including Canadian mobile devices) from being turned into botnets, recommended practices include:

- **Choice of operating system:** some operating systems are known to objectively be far more likely to be compromised than others (see https://www.statista.com/statistics/680943/malware-os-distribution/). Whatever operating system is selected, ensure use of the most recent stable and supported release.
- **Patching:** many botnets exploit known vulnerabilities. If users kept their systems patched up to date, they'd be less likely to become infected.
- **Antivirus:** it is true that malware authors are often adept at avoiding antivirus products, but that's still no excuse for failing to run one. Imperfect though some antivirus products may be, they still add another layer of protection and will block some attack attempts.
- **Strong and unique passwords with two factor authentication:** If a user picks a weak/easily guessable password, or uses the same password at multiple sites, they increase the likelihood that they're going to end up botted. Use of a password manager facilitates the use of strong, unique passwords for each site (www.m3aawg.org/Password-Managers-BP). Use of two factor authentication is the other key to preventing most other account takeovers (www.m3aawg.org/multifactor-authentication-bp).
- **Firewall:** Many home network gateway devices combine a firewall with a wireless access point. While that sort of firewall cannot block all external attacks, it will at least normally defeat many

simple mass scanning attacks. Naturally, the wireless access functionality should also be securely configured, and the wireless access point itself should also be kept patched up-to-date.

- **Block Malvertising:** Malicious advertising is known to be a popular potential attack channel. Blocking most (or all) advertising may help reduce a user's exposure to malvertising.
- **Use a Security-Focused Internet Service Provider:** Choosing a security-focused ISP means that if you do get compromised, your ISP may have the ability to detect that compromise and promptly notify you (other ISPs may consider any compromise to be your problem, not theirs).

If the goal is to deter Canadians from being ATTACKED by bots, consider three common bot-based attacks:

Consideration: In the case of distributed denial of service ("DDoS") volumetric attacks perpetrated by bots, many times those attacks leverage emission of spoofed traffic. Providers should filter spoofed traffic attempting to use source IPs that don't belong to that provider (known as "Source Address Validation,"
https://www.manrs.org/isps/guide/antispoofing/).

Consideration: DDoS attacks using DNS is an attack vector whereby the attackers leverage poorly managed open DNS resolvers that respond to unlimited amounts of queries sent by any Internet user. ISPs and mobile carriers should manage their DNS resolvers by implementing good rate-limiting policies that would prevent them from being used as attack vectors against others.

Consideration: Another popular use case for bots is sending spam. As long as providers in random international locations allow consumers to send email traffic directly to port 25, Canadian email users and Canadian mail service providers will continue to see spam sent via bots. Providers should require traffic to go through the mail server the provider has established for customer use.

Consideration: Regarding Call for Comments Paragraph 42-43, *"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. 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."*, recursive resolver service is a critical element of offering Internet service. If a customer's recursive resolver doesn't work, as far as the customer's concerned, "The Internet is down." For that reason, most ISPs deploy and operate their own farm of recursive resolvers for their customers 'use. These recursive resolvers are normally provisioned as part of the user getting an IP address via DHCP.

Consideration: In addition to controlling whether or not an ISP appears to be up and stable, recursive resolver speed can also be critical to a user's assessment of "ISP performance" -- when a customer complains that "the Internet is slow," they may actually be seeing poor performance from a remote or overloaded alternative recursive resolver they've selected.

Consideration: A user can opt into a third party recursive resolver through a variety of different ways -- for example, the user might modify the recursive resolver configured into their home gateway, in which case all hosts using that home gateway are potentially protected -- but only when those devices are behind that home gateway, not when they're roaming and connecting at work, or while using a

restaurant's WiFi while getting lunch. Conversely, a user might hard code the use of a third party resolver directly into their laptop or WiFi-connected tablet, but when doing that, it's easy to miss one or more devices, particularly in a family situation. This may sound like a minor matter, but if a botnet can get a toe hold on ANY device on a local network, it can then use that infected system as a base from which to attack all the other systems on that local area network.

Consideration: The role of DNS Over HTTPS or DNS Over TLS. While electing to use a third party recursive resolver may potentially result in some malware getting blocked, if the user accesses the third party recursive resolver via an encrypted connection (DOH or DOT), and does get infected, their ISP may not be able to detect that and notify the user since all DNS telemetry is being diverted to a non-ISP destination. See the more extensive discussion available in:

- "M3AAWG Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic," https://www.m3aawg.org/dns-crypto-tutorial, and
- "M3AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic," https://www.m3aawg.org/dns-crypto-recipes.

Thank you for the opportunity to comment on this important initiative.

Sincerely,
Amy Cadagin
Executive Director
M3AAWG - Messaging, Malware, Mobile Anti-Abuse Working Group