Model code of conduct on mitigating botnets and infected machines

E Silva, Karine; Koops, Bert-Jaap; van der Sloot, Bart

Model Code of Conduct on mitigating botnets and infected machines

Background

This document presents a model Code of Conduct (CoC) on botnet mitigation, which can be used by private parties as a self-regulatory instrument and/or by parties collaborating in Public-Private Partnerships. This model CoC was developed in the context of the BotLeg project,[1] to facilitate public-private collaboration in the field of cybersecurity, in particular actions focused on preventing and combating botnets and infected machines.

This document comprises key components of a Code of Conduct, or statement of Best Practices, that participants can adopt in order to clarify their commitment to mitigating botnets and infected machines. The components can be reformulated, refined, and elaborated where desirable, for instance with a view to the specifics of a sector, jurisdiction, or type of organization in which the participants are active.

[1] Project *Public-private actions against botnets: establishing the legal boundaries (BotLeg)* (2014-2018), coordinated by Tilburg University, funded by the Netherlands Organisation for Scientific Research (NWO), project number 628.001.015.
[2] https://creativecommons.org/licenses/by-nc-sa/4.0/

Table of Contents

Preamble

Given that botnets constitute networks of infected devices compromised by advanced software and that such botnets can be used to launch powerful cyberattacks,

Given that botnets are managed by bot-masters (a.k.a. bot-herders), who influence the common communication channels between the devices and are thus capable of manipulating the operations of such devices,

Seeing that the power acquired by bot-masters is reflected in the size and resilience of the botnet, which can be used to perform further criminal acts,

Seeing that botnets are very lucrative, generating income via a multitude of cybercrimes, such as data copying, spam, search engine poisoning, extortion demands through DDoS attacks and ransomware, and click fraud,

Recognizing that botnets are complex, resilient infections that often remain under the radar of security tools such as firewalls and anti-viruses,

Recognizing that with no clear sign that a device is contaminated, users are generally unaware that their devices are infected,

Recognizing that recent industry reports revealed botnet infections affect 500 million computers every year, at a rate of 18 victims per second,

Agreeing that botnets are among the most serious threats to information security,

Agreeing that a coordinated approach to botnet mitigation and control are called for,

Agreeing that cooperation and information sharing are key assets,

The participants to this Code of Conduct agree on the following

A. Scope

A.1 Voluntary agreement

The Code of Conduct ('CoC') is a voluntary agreement set by Internet Industry representatives in [*jurisdiction/sector*] and shall serve as a guide to its participants.

A.2 Shared responsibility

Participants hereby recognize that cybersecurity is a shared responsibility and that each Internet Industry actor should do what they can to contribute to increased security.

A.3 Promoting private and public good

Participants hereby recognize that they have a role to play in countering botnets affecting their services and clients and may contribute to the collective good by protecting the Internet from cyber threats.

A.4 Definitions

Botnet: for the purposes of this Code of Conduct, a botnet is understood as a connected network of machines infected by malware that enables some form of remote control over the infected machines.

Prevention: for the purposes of this Code of Conduct, prevention shall mean the collection of technical, legal, and policy-oriented measures deployed with the purpose of preventing the creation, expansion, and use of a botnet.

Information sharing: for the purposes of this Code of Conduct, information sharing will mean the swift exchange of data related to botnets within a trusted, centralized or hybrid environment, where architecture mechanisms enable fast intelligent data analysis, data input, output, and usage controls, compliance with the law, and minimization of liability concerns.

Disruption: for the purposes of this Code of Conduct, disruption will mean the set of technical and legal measures undertaken with the purpose of disturbing, interrupting, stopping, or terminating the creation, expansion, or use of a botnet.

Disinfection: for the purposes of this Code of Conduct, disinfection will mean every tool or technology deployed or made available for cleaning a system from an infection by means of removing the bot malware or patching a vulnerability exploited by the botnet.

A.5 Duty of Care

The parties to this Code of Conduct will use their resources, capacities and means to prevent and mitigate harms resulting from botnets when such efforts can reasonably be expected of them, in view of their role, capacity, and the costs involved.

B. Prevention

B.1 Security-By-Design

Participants shall encourage a security-by-design model within their organizations from the early stages of any project and throughout their lifecycle. Participants commit to promoting a culture of security and privacy by default, and to stimulating security from conception to manufacturing.

B.2 Awareness-Raising

Participants commit to carrying out periodic awareness-raising campaigns inside and outside their organization and customer base. These campaigns are dedicated to fostering and promoting a culture of cyber hygiene, raising awareness about botnets.

B.3 Monitoring Tools

Participants commit to put in place, within legal limits, monitoring tools that detect, identify, and report behavior associated with botnets. This can be achieved through active and passive detection.

- *Active detection* of botnets shall comprise every tool or system put in place with the goal of gathering information about a botnet by interfering with its functioning.
- *Passive detection* of botnets shall comprise every tool or system put in place with the goal of gathering information about a botnet without interfering with its functioning.

B.4 Record

Participants will record all preventive measures taken and share this information with other participants of this CoC at the end of every year.

C. Cooperation

C.1 Data collection and storage

Participants will collect and store intelligence on botnets infections and threats on their networks and on the networks of others, where appropriate and in accordance with the law.

C.2 Sharing intelligence

Participants shall share intelligence with other participants upon receiving information about concrete, imminent, or potential threats and about general developments concerning botnets and botnet attacks.

C.3 Information sharing platform

Participants shall contribute to an information sharing platform that facilitates easy, swift and secure data exchange between participants.

C.4 Cooperation with non-CoC participants

The participants will:
- actively participate in relevant other private-private and public-private partnerships,
- collaborate with law enforcement by reporting evidence of botnets to the authorities in a timely manner and by actively contributing to criminal investigations and criminal procedures led by national and foreign authorities in accordance with the law,
- contribute to relevant international consortiums and initiatives in the field of botnet mitigation.

C.5 Record

Participants will record all information sharing activities and share this information with participants at the end of every year.

D. Disruption

D.1 Disruption

Upon receiving intelligence about botnet infections, either through own efforts or through information received, the participants commit to taking immediate steps to disrupt the botnet within their capacities and in accordance with the law.

D.2 Assistance

Where a participant needs the assistance of another participant to disrupt the botnet, that other participant shall provide it where reasonable.

D.3 Limitation

The use of countermeasures against botnets shall be limited to the protection and defense of the legitimate interests of the actor undertaking the measures. If the takedown effort affects third-party networks and infrastructure, the countermeasures should have a minimal impact on their fundamental rights or those of others.

D.4 Third-party disinfection

Where the botnet affects third-party networks and infrastructure, the participants commit to take appropriate measures to mitigate such attacks from affecting their networks, as well as to make disinfection tools available to their own clients and customers through their communication channels (e.g. website, email, SMS), thereby alerting stakeholders about the need to disinfect compromised machines.

D.5 Information

Where disruptive measures are taken and these measures will affect third-party networks and infrastructure, the participants will consult with these parties before taking such measures, where reasonably possible. Only in a case of exigent circumstances will a third party be informed after the countermeasures have been taken.

D.6 Record

Participants will record all disruptive measures and share this information with other participants at the end of every year.

E. Governance

E.1 Coordination

The full group of participants will designate one or more participants as coordinator of the CoC. The coordinator of the CoC shall be chosen by a majority vote. The coordinator shall facilitate the exchange of information between participants and shall oversee the sharing of the yearly reports mentioned under the Record provisions of each pillar. The coordinator can be tasked, upon mutual agreement, with other responsibilities that may facilitate compliance with the CoC.

E.2 Recognition

Participants can agree on a label, seal of approval, or other token of recognition that expresses participation in the CoC.

E.3 Compliance

Participants commit to living up to the activities agreed upon in this CoC. If a participant cannot (any longer) live up to the activities, they can withdraw from the CoC at any moment, provided that they have notified all participants and the coordinator in advance within a reasonable period.

E.4 Non-compliance

In case a participants fails to comply with their commitments under this CoC, the other participants can agree to exclude the non-complying participants from the agreement. Such exclusion can only take place with [*consensus / two-thirds majority*] of the other participants and following an advance warning that includes a reasonable period allowing the non-complying participant to demonstrate (future) compliance. Exclusion shall not take place for issues of non-compliance that are minor in the context of the overall CoC.

Upon exclusion of a participant, the coordinator shall take steps to facilitate that the excluded participant no longer uses the token of recognition agreed upon under E.2.

E.5 Interpretation

The terms of this CoC shall be interpreted in accordance with the mutual understanding of the participants. In case of disagreement over the interpretation of the terms, the participants shall discuss with the aim of arriving at a mutual understanding. If disagreement persists, the coordinator may – having heard all arguments – propose an interpretation that shall be binding if [*a two-thirds majority*] agree with this interpretation. If disagreement still persists, participants may decide to reformulate the contested provision in a manner that does express the mutual understanding of the participants.

E.6 Period of validity and change of terms

This CoC shall be effective for a period of [*two / three / five*] years and be evaluated towards the end of that period. The period may be renewed upon [*consensus / two-thirds majority*] of the participants.

The terms of this CoC can be changed, following a proposal by one or more participants and following a decision by all participants, with [*consensus / two-thirds majority*]. The participants shall agree upon the procedure that needs to be followed for adapting this CoC.