Botnets

An Internet Society Public Policy Briefing

Internet Society

30 October 2015

Introduction

Botnets are a complex and continuously evolving challenge to user confidence and security on the Internet. Combating botnets requires cross-border and multidisciplinary collaboration, innovative technical approaches, and the widespread deployment of mitigation measures that respect the fundamental principles of the Internet.

A botnet is a collection of Internet-connected user computers (bots) infected by malicious software (malware) that allows the computers to be controlled remotely by an operator (bot herder) through a Command-and-Control (C&C) server to perform automated tasks, such as stealing information or launching attacks on other computers. Botnet malware is designed to give its operators control of many user computers at once. This enables botnet operators to use computing and bandwidth resources across many different networks for malicious activities.

Historically, botnets mainly have been used to originate and propagate spam messages. They can be used for many malicious purposes, including to steal personal data and passwords, attack public and private networks, exploit users' computing power and Internet access, and carry out Distributed Denial of Service (DDoS) attacks.[1] In short, botnets are a complex and continuously evolving problem that poses a threat to user confidence in the Internet.

Various techniques are used to infect computers so they become bots, including luring users into downloading malware, exploiting Internet browser vulnerabilities, and tricking users into loading malware (e.g., as a result of opening an infected email attachment). Botnet malware is often designed to run in the background so users are unaware that their systems are infected.

Although botnets pose threats to Internet users and are difficult to eliminate, steps can be taken to reduce their impact and associated risks.

Key Considerations

Botnets impose economic and social costs on affected users, service providers, network operators, and society as a whole. Without effective efforts to mitigate them, botnets have the potential to harm the overall economic and social benefits of

[1] https://en.wikipedia.org/wiki/Denial-of-service_attack

the Internet. A number of issues must be considered when addressing the problem of botnets. These include:

- **Geographic dispersion**. Botnets can be widely spread across distance and geography, with infected computers and botnet herders operating in different countries and locations. Same applies to the C&C servers. As such, botnets are transnational and require a collaborative approach to detection, mitigation, and law enforcement.

- **Impacts on user rights.** It is important to consider the impact on fundamental user rights and expectations when approaching strategies to combat botnets. Overly broad botnet-mitigation strategies, such as blocking all traffic from an infected network, could unintentionally keep innocent users from accessing the Internet and exercising rights, such as freedom of expression and opinion. In addition, some methods to detect and trace botnets, such as the indiscriminate collection of network traffic data, could violate the privacy of legitimate Internet users.

- **Impacts on technology use and innovation.** Some technical and legal mitigation strategies, such as restricting access to suspected infected networks, may have negative consequences on the openness, innovation potential, and global reach of the Internet. Further, technology-specific strategies are less likely to address the overall problem of botnets, as their creators may change tactics to avoid new obstacles.

Challenges

A number of factors contribute to the ongoing challenge of combating botnets, including:

- Botnet strategies, technologies, and techniques are constantly evolving and adapting in response to mitigation measures.

- Botnets have become popular tools for cybercriminals because they are cheap to deploy and operate, hard to uncover, and are available for purchase or rent through criminal networks.[2]

- Botnet creators and herders are geographically dispersed from the offending bots and are skillful at hiding their locations and identities.

- There are vulnerable computers connected to the Internet (e.g., those that are not sufficiently secured or whose users are susceptible to being lured into introducing botnet malware into their computers). Botnet operators actively search for vulnerable systems to infect.

- Botnets are designed to take advantage of the Internet's fundamental properties (the Internet Invariants[3]) and its architectural design, where the

[2] For examples, see http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime and http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/

[3] See Internet Invariants: What Really Matters http://www.internetsociety.org/internet-invariants-what-really-matters

intelligence is in the end devices (e.g., botnet command and control servers and infected computers) rather than the network itself.

Guiding Principles

The Internet Society believes that a collaborative approach among all relevant stakeholders will provide the best botnet-mitigation solutions and security protection. This approach is embodied in the Internet Society's Collaborative Security principles, which emphasize a shared and collective responsibility to achieve desired outcomes.[4] This collaborative security approach comprises the following principles:

Fostering confidence and protecting opportunities. The objective of security is to promote confidence in the Internet and to ensure its continued success as a driver for economic and social innovation.

- *Promote awareness.* Promote the general awareness that stakeholders are committed to working together to take down and discourage the creation of new botnets by effective, efficient, and reasonable measures.

- *Promote safe systems.* Promote a safer Internet-user experience by encouraging secure software design practices, high-quality common security components, timely detection of vulnerabilities, provision of updates, and similar systems.

- *Promote safe devices.* Promote the use of systems that are properly configured to resist botnets. For example, at the individual computer level, the use of malware protection and spyware detection software reduces the risk of botnet infection.

- *Promote containment.* Promote the improvement of the Internet community's overall technical ability to contain the spread, operation, and impact of botnets. This includes improving abilities to deactivate botnets to reduce damage.

Collective responsibility. Internet participants share a responsibility for the system as a whole.

- *Shared responsibility.* Efforts should be made to share the responsibility for addressing botnets across stakeholders, including governments, network operators, software vendors, online service providers, the technical community, and end users. For example, although a network that unknowingly hosts a botnet might not be directly affected, that network operator should be responsible for ensuring that it does not become a launch pad for malicious activity. A "code" for such responsible network management is documented in the "The Anti-Bot Code of Conduct for Internet Service Providers, A Voluntary Industry Code to Help Reduce End-User Bots"[5]. Generally speaking, relying on a few parties to implement botnet policies or artificially imposing legal liability, rather than implementing a

[4] Internet Society's Collaborative Security Principles, http://www.internetsociety.org/collaborativesecurity.
[5] See https://www.m3aawg.org/abcs-for-ISP-code

collective approach, places an unfair burden on some and has the potential to disrupt the shared responsibility model of the Internet.

- *Collaborative approach.* Collaborative activities are essential when dealing with botnets. This includes sharing intelligence and operational attack data, sharing good practices and mitigation methods, and coordinating antibotnet activities. It is also important that collaboration be proactive and not reactive.

- *Cross-border enforcement.* Cross-border collaboration can be facilitated by laws that make botnets and their malicious activity illegal and permit appropriate information collection and sharing for mitigation and enforcement. Careful thought should be given as to how technical measures that detect and mitigate botnets across borders are implemented, who is involved, and what is reasonable and permissible.

Fundamental properties and values. Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet, the Internet Invariants.

- *Respect user rights.* Policy approaches should take into account the potential unintended effects on user access and privacy when implementing actions to address botnets. Well-intentioned solutions to botnets might inadvertently hurt legitimate uses of the Internet or unnecessarily expose private user information.

- *Preserve the fundamental properties of the Internet.* Policy approaches should take into account the potential impact on the underlying architecture of the Internet and ensure that they do not negatively impact the openness, permissionless innovation, or global reach of the Internet. For example, taking down a domain might inadvertently render legitimate uninfected websites unreachable.[6]

Evolution and consensus. Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.

- *Agility.* Policies and solutions should be agile enough to remain effective given the rapid evolution of botnets. For example, policies that prevent security researchers from investigating botnet behavior might delay the development of new antibotnet tools and techniques. Further, policies should strive to address the creation, propagation, and functioning of bots and command and control servers, as well as the individuals who own and operate them.

- *Technology-neutral solutions.* Long-term approaches should be designed to be technology neutral, meaning they do not prescribe a detailed technical solution. Instead, solutions should specify a general strategy, thereby enabling the detailed implementation to be adaptable to new technologies.

[6] See, for example, http://www.pcworld.com/article/2452460/microsoft-settles-with-noip-in-botnet-hunt-after-seizing-its-domains.html

- *Focus on root causes.* Strategies should focus on addressing the root cause of the problem. Addressing symptoms (e.g., spam) without also addressing the root cause (the botnet) may neglect other malicious botnet activities (e.g., theft of personal data).

- *Partial solutions.* Policy makers should consider that partial solutions for combatting botnets might have merit. Incremental measures of detecting and deactivating botnets do not eliminate the threat completely, but they do help contain the problem and erode the profitability of botnets.

Think globally, act locally. The most effective solutions are likely to be reached via bottom-up self-organization.

- *Build trust.* Generally, the most effective strategies against botnets are implemented by informal self-organizing groups that are built on trust among experts in the field.[7]

Additional Resources

The Internet Society has published a number of papers and additional content related to this issue. These are available for free access on the Internet Society website.

- *Collaborative Security: An approach to tackling Internet Security issues,* http://www.internetsociety.org/collaborativesecurity.

- Global Multi-Stakeholder Collaboration for Achieving a Safe, Secure, and Tolerant Cyberspace: Enabling Growth and Sustainable Development through Cyber Ethics, http://internetsociety.org/doc/global-multi-stakeholder-collaboration-achieving-safe-secure-and-tolerant-cyberspace-enabling.

- Understanding Security and Resilience of the Internet, http://www.internetsociety.org/doc/understanding-security-and-resilience-internet and infographic: Collaboration for a secure and resilient Internet, http://internetsociety.org/doc/infographic-collaboration-secure-and-resilient-internet.

- Cybersecurity: Laying Out Pieces of the Cybersecurity Puzzle, http://internetsociety.org/cybersecurity-laying-out-pieces-cybersecurity-puzzle.

- *Towards Improving DNS Security, Stability, and Resiliency,* http://internetsociety.org/towards-improving-dns-security-stability-and-resiliency-0.

[7] See for example, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836