First Look: Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Outlines future goals and suggested actions by the US Departments of Commerce and Homeland Security to mitigate cybersecurity threats to industry and society.

Updated last June 12, 2018 for the 05/20/2018 version of the report.

WHAT IT DOES

“Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats” is a report outlining future goals and suggested actions by the US Departments of Commerce and Homeland Security to mitigate cybersecurity threats to industry and society.

After consideration of public comments and consultation with the Departments of Defense, Justice, and State; the Federal Bureau of Investigation; the Federal Communications Commission; the Federal Trade Commission; and the President’s National Security Telecommunications Advisory Committee, the authors of this report established six themes describing the opportunities and challenges regarding botnets and cybersecurity. They are:

1. Globality of Botnets - Recent examples of botnet attacks on US communications systems indicate that attacks come from adversarial or compromised devices located around the globe. International partnerships will be necessary to effectively mitigate these international cybersecurity threats.
2. Lack of Common Practices – Select sectors of the market and government have effectively implemented tools to prevent or combat cyberthreats, however the use of these tools has yet to become an accessible and common practice for all key stakeholders.
3. Lifecycle Security – Cyberthreats can evolve and persist throughout the lifecycle of any technology. Frequent security monitoring and updates are necessary.
4. Awareness and Education – Consumers and producers of devices are key players in ensuring that their devices are not compromised for a botnet attack. Device developers, manufacturers, and infrastructure providers can help educate users of the best practices for securing their devices.
5. Misaligned Market Incentives – Currently, the producers, manufacturers, and infrastructure providers lack adequate incentives to promote their participation in mitigating cybersecurity threats. Incentives for these stakeholders could be realigned to support their cooperation and leadership.
6. Ubiquitous Challenges – Cybersecurity threats presented by botnets affect all participants in the communications ecosystem. All communications stakeholders’ joint participation will be required to effectively mitigate the threat of botnets.

The report also includes five goals and 24 suggested actions (some already in effect) to accomplish each goal for the stakeholders indicated above. These goals are:

- Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure marketplace for devices susceptible to being compromised for botnet attacks.
- Goal 2: Promote innovation in the communications infrastructures to support susceptible devices.
- Goal 3: Promote innovation at the edge of communication networks to prevent, detect, and mitigate automated, distributed
attacks.

- Goal 4: Promote and support coalitions between the security, infrastructure, and operational technology communities around the world.
- Goal 5: Increase awareness and education across the communications ecosystem to help mitigate botnet threats.

The report also indicates that the Federal Government will take the lead in implementing and supporting the following measures:

- Developing a road map and private-sector leadership to help coordinate efforts to mitigate botnet risks to cybersecurity;
- Providing a 365-day status report to the President on road map implementation;
- Promoting global participation in cybersecurity threat mitigation through policy and standards development with international stakeholders; and
- Leading by example by improving federal education of cybersecurity threat deterrence and secure device acquisition efforts.

RELEVANT SCIENCE

The term botnet refers to groups of automated devices (computers, mobile phones, Internet of Things devices) connected over a communications network that are controlled by a single operator to work in conjunction and perform a task with the combined computational power of the networked devices. Botnets are created and controlled through the introduction of a program on any device that then is downloaded on other devices connected to the original device’s network. In malicious botnets, the controlling program often infects vulnerable devices as a virus without the knowledge of the device’s owner. Once compromised, a device’s data and functioning can be susceptible to the agent controlling the botnet. Examples of botnet use can be found [here](https://example.com).

STATUS

This report was created in response to the May 11, 2017 Executive Order, “Strengthening the Cyber Security of Federal Networks and Critical Infrastructure”, directing the Departments of Commerce and Homeland Security to establish an open process for identifying and mitigating the threat of adversarial botnets to the internet and other communications systems. The report’s publication was first announced to the public for comment on January 5, 2018 following an initial inquiry and workshop hosted by the President’s National Security Telecommunications Advisory Committee (NSTAC). The revised and finished report was published to the public on May 20, 2018.

As indicated above, the report outlines four immediate steps that the Departments of Commerce and Homeland Security will pursue. A full report on their efforts will be provided to the President in one year.

PRIMARY AUTHOR

Scott "Esko" Brummel, MA in Bioethics and Science Policy

RECOMMENDED CITATION


LICENSE
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. Please distribute widely but give credit to Duke SciPol, linking back to this page if possible.