July 28, 2017

Joint comment from the Internet Society and the Online Trust Alliance on the National Telecommunication and Information Association's

Request for Comments on Promoting Stakeholder Action against Botnets and Other Automated Threats

Docket No. 170602536-7536-01

The Internet Society and the Online Trust Alliance (OTA) are pleased to submit these joint comments in response to NTIA's Request for Comments on Promoting Stakeholder Action against Botnets and Other Automated Threats. The Internet Architecture Board, a body within the Internet Engineering Task Force (IETF), has independently submitted a response referring relevant material from the IETF on specific technical aspects surrounding botnets and other automated threats.

Fundamentally, botnets and automated threats are enabled by vulnerabilities resulting from unpatched servers, websites hosted with vulnerable plugins and modules, and compromised devices (including PCs) that can be exploited remotely. Furthermore, the vast and increasing numbers of insecure Internet of Things (IoT) devices present a growing environment for developing botnets and other automated threats. Already, vulnerabilities in IoT devices have been used to inflict harm on Internet users, whether it be through privacy breaches or distributed denial of service (DDoS) attacks and other forms of automated threats. Bots also drive fake news and click fraud, influencing physical world institutions and online business models. To mitigate these threats, the Internet Society and the OTA propose the following:

1. Reduce the attack surface or the number of vulnerable devices connected to the Internet.
2. Reduce the ability of attackers to control devices.
3. Limit the effect of any attacks originating from devices.

The Internet Society and the Online Trust Alliance recognize that addressing the threats and impact of botnets requires a collaborative approach and shared responsibilities. This work has been the foundation of the OTA/ISOC Internet of Things Trust framework, a set of core security, privacy and sustainability principles.[1] [2] The framework aims to drive the adoption of these principles by design. It is a voluntary, but enforceable, code of conduct and provides positive affirmation and recognition to companies, products, and retailers who embrace the code of conduct and meet minimum standards. The framework works as both as an incentive

[1] OTA IoT Trust Framework https://otalliance.org/IoT

[2] OTA Securing the Internet of Things; A Collaborative & Shared Responsibility https://otalliance.org/Vision

internetsociety.org
@internetsociety

Galerie Jean-Malbuisson 15,
Geneva, CH-1204 Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

1775 Wiehle Ave, Suite 201,
Reston, VA 20190 USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

and educational tool for IoT device and service developers. The comments below are, in part, based on this Trust Framework and the Internet Society's Collaborative Security Framework.[3]

A list of best/promising practices identified by the Internet Society and the OTA is included in an Appendix to this comment.

1. **Reducing the attack surface through addressing IoT security**

Collaborative actions are necessary to better secure IoT devices and services, however with little incentive and a lack of resources, these actions have yet to be widely adopted. For device manufacturers and service providers, there is currently little incentive to secure their products. For example:

- There are few direct financial impacts from unsecure devices; good security is expensive.
- There is a need to get products to market quickly; and, since consumers are often unable to tell good security from bad security, there is little market incentive for better security.
- Some device manufacturers and service providers, particularly those that are new to the Internet ecosystem, do not have the resources needed to build stronger security.

For users, a general lack of resources limits their ability to secure their products or influence the market. There is no recognized certification for IoT security. For example:

- Consumer organizations have not yet begun testing IoT security in their review processes, making it difficult for users to determine the level of security of the products they buy.
- There is also no single source to discover remediation resources. It is important to note that some question whether users should be expected to be involved in remediation at all, as even highly-educated customers that care find it hard to determine if tools are trustworthy, where they should turn, and what tools to use.
- Users may not know how to patch or take other precautions to mitigate the threat of malware on their devices.

All stakeholders, including governments, need to take actions to better secure IoT devices and services. They should:

- Recognize their shared responsibility for securing the Internet ecosystem.
- Incentivize better security practices:
    - Governments should create a market for security through their own procurement practices.
    - Governments should clarify the applicability of existing consumer protection and data privacy regulations to IoT.

[3] Collaborative Security: An approach to tackling Internet Security issues https://www.internetsociety.org/collaborativesecurity

    - Regulation or legal requirements must be carefully formulated, through ongoing conversations with stakeholders, to not stifle innovation.
    - Consumer organizations should develop testing standards to review security on IoT products, creating better resources for consumers to use when buying products.
    - Industry should develop voluntary security norms and promote adoption.
- Develop or promote better IoT security practices:
    - Engage in collaborative efforts to develop technology-neutral solutions to challenges in IoT security.
    - 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.
    - Foster 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.
    - Support user awareness programs to educate users on strong security practices.
- Take into account global context, and the ongoing efforts in other countries, international organizations, and standards development organizations.

2. Reducing the ability of attackers to control devices

The ability of attackers to control devices must be reduced. Coordinated international efforts are critical to target and deactivate the command and control (C&C) servers of botnets and other automated threats. Actions must also be taken to improve 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.

3. Mitigating the impact of botnets and other automated attacks

Finally, efforts must be made to mitigate the impact of botnets and other automated attacks. The Internet Society and OTA recommend the following actions:

- Enhance 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.
- Support law enforcement efforts, including botnet take-downs, while taking into consideration the risk to collateral damage to innocent third parties, errors in identifying targets for mitigation and respecting users' privacy.
- 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.
- Work with international partners to mitigate the impact of botnets and facilitate cross-border enforcement. Laws that make botnets and their malicious activity illegal and

permit appropriate information collection and sharing enable 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.

- Support trusted communities, like Computer Security Incident Response Teams (CSIRTs) and Information Sharing and Analysis Centers (ISACs), which enable information sharing related to threats and observed incidents.

About the Internet Society and Online Trust Alliance

The Internet Society is a global not-for profit organization committed to the open development, evolution and use of the Internet for the benefit of all people throughout the world. Working in partnership with our global community, comprised of nearly 100,000 members, 123 chapters, as well as more than 160 organizational members. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF) and the Online Trust Alliance (OTA).

The OTA is an initiative within the Internet Society (ISOC) with a mission to enhance online trust, empower users' innovation through convening multi-stakeholder initiatives, and to develop and promote best practices, ethical privacy practices and data stewardship.

Appendix 1

The Digital Standard is an open and collaborative effort to create a digital privacy and security standard. While the Standard will act as a guide for companies in the design of mobile and Internet-connected products and services, it will also enable Consumer Reports and other testing organizations to have criteria by which to test, evaluate, and report on the security and privacy of products. The initiative is spearheaded by Consumer Reports, The Cyber Independent Testing Lab, Ranking Digital Rights, Aspiration and Disconnect. The Digital Standard, and testing by consumer organizations, can help educate consumers on IoT security, building market forces for better security.[4]

The Shadowserver Foundation, an independent non-profit organization, tracks botnets and establishes client sessions directly to the C&C server. Shadowserver's custom software then logs the botnet's traffic without performing malicious activity. Shadowserver does not attempt to shut down the botnet on their own. After gathering enough incriminating evidence, Shadowserver collaborates with relevant law enforcement agencies and service providers to shut down the botnet.[5]

The Conficker Working Group was an informal multistakeholder group of experts organized to stop computers infected by the Conficker malware from reaching out each day to the botnet's C&C controllers. The group would register and block domains before the Conficker author, stopping the author from updating the botnet.[6]

The Mutually Agreed Norms for Routing Security (**MANRS)** were developed by several network operators with the Internet Society to create clear baseline security requirements and visible commitment among Internet service providers to make routing safer. It defines common principles to adhere to and four concrete actions for network operators to take. One of the actions, to prevent traffic with spoofed source IP addresses, helps mitigate amplification techniques used in some forms of DDoS attacks. MANRS network operators commit to the initiative's principles and implement the majority of its four defined actions. MANRS builds a culture of collaboration and security among participants. Members may display the MANRS symbol on their sites and are listed on the MANRS website. Thanks to peer pressure and leveraging MANRS as a market force, the community has grown to over 160 networks.[7]

Farsight Security, a DNS security company, is just one example of a private organization engaging in efforts to protect its customers from automated threats. Farsight Security's efforts include using a Passive DNS sensor array and DNS historical database to detect new domains. As new domains are sometimes used for criminal purposes, Farsight Security will

[4] The Digital Standard: https://www.thedigitalstandard.org/
[5] The Shadowserver Foundation: https://www.shadowserver.org/wiki/pmwiki.php
[6] The Conficker Working Group: http://confickerworkinggroup.org/wiki/
[7] Mutually Agreed Norms for Routing Security (MANRS): https://www.routingmanifesto.org/manrs/

quarantine the domains' interactions with their customers until enough time has passed to classify them as safe. This helps prevent their customers, if infected as part of a botnet, from connecting to new domain names which may contain a C&C server.[8]

The Underwriters Laboratories' Cybersecurity Assurance Program (known as UL CAP) offers testable cybersecurity criteria for network-connectable products and systems to increase their safety. UL CAP is for vendors seeking security risk support and purchasers seeking to mitigate risk by purchasing products validated by a third party.[9]

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit that offers unbiased information on best practices to increase software security.[10] All of OWASP's materials are available under a free and open software license to anyone who wishes to access it. OWASP's Internet of Things Project is designed to help all stakeholders understand IoT security issues and promote the secure building, deployment, and assessing of IoT technologies.[11]

[8] Farsight Security: https://www.farsightsecurity.com/
[9] Underwriters Lab Cybersecurity Assurance Program (UL CAP): http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/
[10] Open Web Application Security Project (OWASP): https://www.owasp.org/
[11] OWASP IoT Project: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project