July 28, 2017

National Telecommunications and Information Administration
United States Department of Commerce
Washington, DC
Email: counter_botnet_RFC@ntia.doc.gov

RE: Infineon Technologies Americas Corp. Comments on “Promoting Stakeholder Action Against Botnets and Other Automated Threats”

Docket Number: 170602536-7536-01

Dear NTIA,

Infineon welcomes the efforts by NTIA to promoting increased security on the internet and is glad for the opportunity to add comment from the perspective of a secure hardware provider. Infineon Technologies is a leader in the design and production of secure integrated circuits applied in embedded applications of devices and systems. When devices become connected, the availability, integrity and confidentiality of the devices and the messages that they send and receive need to be protected. With decades of experience in delivering hardware security for critical applications segments like payments, communications, government identification, transportation, and PayTV to systems and devices such as servers, routers, Automated Teller Machines (ATMs), phones, and set-top boxes, Infineon has substantial expertise and know-how in secure technology, process and best practices for securing embedded systems and deploying solutions globally.

1. *What works?:*

Previous mitigation efforts by public and private stakeholders like identifying and sinkholing malicious traffic have had some effect in reducing botnet activity. However, the problem continues to grow in spite of these efforts.

2. *Gaps:*

The rapid increase in IoT devices changes the nature of the threat. With millions of unattended devices connected to the Internet (directly or indirectly), criminals have discovered that a tidy profit can be made by building a botnet and renting it out for DDoS attacks.[1]

The real problem to solve in mitigating the impact of botnets is insecure devices. We can’t build a safe Internet out of insecure devices.

5. *Policy and the role of government:*

NTIA should continue to convene stakeholders from the technology, policy, and consumer sectors to develop state-of-the-art guidelines and recommendations for securing the Internet. Further, NTIA should continue its collaboration with the private sector to design both incentives and disincentives to encourage device manufacturers to adopt best practices for IoT.

Industry organizations including the IoT Security Foundation, the Industrial Internet Consortium, and the Trusted Computing Group each have developed and are developing standards and guidelines for securing devices on the internet:

- The IoT Security Foundation’s Best Practice Guidelines for Connected Consumer Products[2] describes the threats faced by modern IoT devices and lays out recommended best practices for defending such devices.
- The Industrial Internet Consortium’s Industrial Internet Security Framework[3] provides a complete overview of countermeasures relevant to Industrial IoT devices.
- The Trusted Computing Group’s Guidance for Securing IoT Using TCG Technology[4] describes how hardware security can be used to establish highly secure IoT systems.

These guidelines and best practices can serve as a basis for establishing norms in this area.

NTIA’s recent efforts on patching and upgradability are especially helpful because regularly installing software updates is essential to securing devices over time, and secure hardware trust anchors facilitate that capability. Infineon encourages NTIA and other government agencies to continue work on advancing the state of the art in IoT security through multi-stakeholder working groups.

Resilience, including the ability for IoT devices to recover from attack, is another aspect to preventing the widespread consequences of botnets on the internet. As experts in the use of hardware-based security, Infineon is happy to contribute to such efforts.

[1] https://www.scmagazineuk.com/mirai-botmaster-behind-deutsche-telekom-router-hijack-pleads-guilty/article/676906

[2] https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

[3] https://www.iiconsortium.org/IISF.htm

[4] https://trustedcomputinggroup.org/guidance-securing-iot-using-tcg-technology-reference-document/

6. *International:*

Because the Internet and the IoT are international in scope, U.S. Government efforts in this area should be coordinated with the efforts of other nations to avoid conflicting policies. The work of European public and private sector experts on European Baseline Requirements for Security and Privacy[5] may be especially of interest. Infineon is involved in this effort and could help to arrange conversations with the European team.

In summary, we must raise the floor for IoT security by establishing some minimum expectations while rewarding those who exceed those expectations. The best practice guidelines cited here should serve as the basis for those expectations.

Sincerely,

Stephen R. Hanna	Shrinath Eswarahally
Senior Principal, Technical Marketing	Senior Staff Engineer, Applications Engineering
Infineon Technologies Americas Corp.	Infineon Technologies Americas Corp.

[5] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity