NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

February 9, 2018

Dear Sir/Ma'am,

It is a great pleasure to have an opportunity to submit comments to DRAFT FOR PUBLIC COMMENT of "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" (hereafter "DRAFT").

NTT participated in the workshop hosted by NIST in July 2017. NTT also submitted comments to RFC by NTIA in July 2017. The comments in the attachment are built on what we learned from those activities as well as recent progress we observe in the US, Japan and other countries. They are structured with an Executive Summary followed by detailed full comments.

As a global ICT service provider, we commit to contribute to building global cyber resiliency. Since we have sizable businesses in the US, we also commit to contribute to US-based public-private cyber security initiatives. With such commitment, we hope to be a part of the processes and work going forward against botnets and other automated, distributed threats.

Sincerely Yours,

Shinichi Yokohama
Head, Cyber Security Integration
NTT Corporation

Attachment

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Executive Summary

Overall, the DRAFT is right on the spot. Global eco-system collaboration enabled with market incentives is essential.

We think 6 Principal Themes capture the essential nature of the botnet challenges. In particular we concur with the necessity of devising market incentives that cut across different multi-disciplinary communities across the global eco-system. We think 5 Goals and 23 Actions cover most of the key challenges and will initiate substantial positive impact against botnets. Needless to say, sustained execution commitments by key players in the eco-system are imperative for the success of the efforts. In particular, as often noted in the DRAFT, global participation and collaboration is critical.

The DRAFT has lots of commonality to the efforts that are undertaken or under consideration in Japan. There may be good opportunity for US-Japan collaboration.

We find the contents of the DRAFT are very similar to recent government policies and industry initiatives being proposed and discussed in Japan. We understand a few collaborative initiatives have already started between US and Japan, and there may be a good chance to expand the collaboration between two countries both at government level and industry level.

Additional actions may be needed to address challenges caused by the billions of devices that are currently in the market and in use, many of which may be vulnerable and infected already.

As for the 23 Actions proposed in the DRAFT, there may be a couple of additional actions that may be worth consideration. It is our impression that 23 Actions are trying to address challenges generated by future bots, i.e. devices that come to the market and become bot from now. However, we need to address challenges caused by billions of devices that are already in the market, in use and may have been infected already. Also there are a few Actions that are legitimate and worth pursuing, but may not lead to our objectives effectively (for example Action 3-4 on IP v6).

NTT is willing to participate in some of the Actions around Infrastructure. As Actions become clearer, we may also be interested in others such as secure software and enterprise network development.

As a global ICT service provider with sizable business activities in the US, we not only

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

commit to contribute to global cyber resiliency build-up but also we are willing to participate in some of the actions raised in the DRAFT around Goal 2 Infrastructure. We also find some actions in other Goals, such as secure software development, may have relevancy for our efforts to provide security to our clients, and we may be interested in joining them once specifics become clear.

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Full Comments

Overall, the DRAFT is right on the spot. Global eco-system collaboration enabled with market incentives is essential.

We think 6 Principal Themes capture the essential nature of botnet challenges. In particular we concur with the necessity of devising market incentives that cut across different multi-disciplinary communities across the global eco-system. We think 5 Goals and 23 Actions cover most of key challenges and will initiate substantial positive impact against botnets. Needless to say, sustained execution commitments by key players in the eco-system are imperative for the success of the efforts. In particular, as often noted in the DRAFT, global participation and collaboration is critical.

- NTT provides IP backbone service across the world. As a global Tier 1 provider, we have been observing threats in the Internet over a decade. Recently, we observe ultra-scaling of DDoS and IoT attacks generated by Asia and other regions.
- Between 2007 and 2012, the largest DDoS size was double-digits Gbps. In 2016, the largest DDoS was 800 Gbps which is sixteen times larger than 2012. The number of large scale DDoS attacks has also increased. In 2013, there were 39 DDoS attacks which were over 200 Gbps. In 2016, the number has increased to 645.
- Our Global Threat Intelligence Center (GTIC) analyzed that 60% of IoT attacks came from IP addresses within Asia. GTIC also analyzed 60% of NTT Security's detection of Mirai, the IoT botnet, showed source IP address in Asia. The most likely reason for the high volume of attacks coming from devices in Asia is that the products in the Asian market have historically been shown to be vulnerable to compromises and subsequent reuse in attacks.
- It is our belief that collaboration among all stakeholders across national borders, including Asia, is indispensable for enhancing our ability to reduce botnet threats. For example, Tokyo is going to host Olympic and Paralympic Games in 2020. To protect such an important international event from botnet threats, collaboration among all stakeholders is necessary. It is NTT's commitment to contribute to such efforts.

The DRAFT has lots of commonality to the efforts that are undertaken or under consideration in Japan. There may be good opportunity for US-Japan collaboration.

We find the contents of DRAFT are very similar to recent government policies and

industry initiatives being proposed and discussed in Japan. We understand a few collaborative initiatives have already started between US and Japan, and there may be a good chance to expand the collaboration between two countries both at government level and industry level.

- Regarding Infrastructure, an industry-driven working group released a report draft on measures against DDoS attacks to ensure better Internet environment in Japan in December 2017. The report includes three basic principles below.
  - ISPs' potential preventive measures against DDoS attacks
  - Information sharing among ISPs and stakeholders
  - Measures for vulnerable terminal equipment including IoT devices
- Regarding Edge, IoT Acceleration Consortium co-hosted by Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy and Trade Industry (METI) issued IoT Security Guidelines ver.1.0 in July 2016. (http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf) The Consortium has 3,397 Japanese companies as a member (As of Dec. 2017). The Guideline suggests five guiding principles of IoT security measures.
  - Policy: Establishing a basic policy with consideration of the nature of the IoT
  - Analysis: Recognize risks on IoT
  - Design: Considering a design to protect what should be protected
  - Implementation and Connection: Consider security measures on the network side
  - Operation and Maintenance: Maintaining a safe and secure state and disclose and share information
- Regarding Coalition and Education, MIC's Comprehensive IoT Security Measures (Oct. 2017) suggest below initiatives.
  - Measures on IoT devices vulnerabilities
  - R&D promotion
  - Support for the private sector
  - Human resource development
  - International cooperation
- ICT-ISAC Japan* and Comm-ISAC/IT-ISAC in the US have already started collaboration such as The International Workshop on ISAC Collaboration held in Tokyo in November 2016 and 2017. (*See the URL below about ICT-ISAC Japan. https://www.ict-isac.jp/english/index.html#Message)

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

Additional actions may be needed to address challenges caused by the billions of devices that are currently in the market and in use, many of which may be vulnerable and infected already.

As for the 23 Actions proposed in the DRAFT, there may be a couple of additional actions that may be worth consideration. It is our impression that 23 Actions try to address challenges generated future bots, i.e. devices that come to the market and become bot from now. However, we need to address challenges caused by billions of devices that are already in the market, in use and may have been infected already. Also there are a few Actions that are legitimate and worth pursuing, but may not lead to our objectives effectively (for example Action 3-4 on IP v6).

These efforts include introducing more robust data and quantum level security and real-time AI based user behavior analytics. It is important to be able to track data movement both horizontally and vertically. It can consume, analyze, track, control and ultimately secure today's "big data" flowing through networks due to the exponential growth of smart devices as part of the Internet of Everything trend.

- On top of information sharing among ISP's, operation sharing and standardization is important to realize effective collaboration among ISP's. We offer DDoS mitigation service as a Global IP Network (GIN) operator today and announce that we plan to provide "Multi-DDoS mitigation service" in the future, which can protect clients and services from larger-scale DDoS attacks by coordinating with other global ISPs. Automatic and real-time cooperation is ultimate goal and operation sharing and standardization is essential among them.
- Scenario planning to mitigate vulnerable products already deployed/installed in the field may be needed. A specific action example, which is in "A Comprehensive Package of IoT Security Measures," is vulnerability assessment of IoT devices on the Internet by wide-area network scanning. Actually, in August 2013, network scanning was conducted by Telecom-ISAC Japan, the predecessor of ICT-ISAC Japan established in March 2016, to estimate the number of devices in Japan that could be used as stepping stones. Efforts have been put into reducing the number since then.
- It is our thought that IPv6 described in the Action 3.4 may help identify infected products, but all security issues cannot be solved simply by using IPv6. When IPv6 function is implemented to network products, some new security issues may come out depending on network architecture and design. Also, we should consider security issues under the coexistence environment of IPv4 and IPv6 for gradual

transition. In Japan, we operate Next Generation Network (NGN) infrastructure to which IPv6 can be fully applied. Almost all major ISPs utilize IPv6 on the NGN in Japan. According to IPv6 Promotion Council, the penetration rate of IPv6 for "FLET'S Hikari Next," NTT's high-speed optical access service based on NGN, reaches approximately 40% (As of Sep. 2017).

- There seems to be some potential action ideas to be considered. Examples are shown below.
  - Scanning all devices and data and creating an inventory of digital assets to start gaining "control" of existing devices/ data
  - Establish learning loop triangulating audit logs, device behavior analytics tied to possible identities
  - Triangulation of device, user and data
  - Alignment to NIAP, FIPS (140-2) compliance and other similar standards

NTT is willing to participate in some of the Actions around Infrastructure. As Actions become clearer, we may also be interested in others such as secure software and enterprise network development.

As a global ICT service provider with sizable business activities in the US, we not only commit to contribute to global cyber resiliency build-up but also we are willing to participate in some of the actions raised in the DRAFT around Goal 2 Infrastructure. We also find some actions in other Goals, such as secure software development, may have relevancy for our efforts to provide security to our clients, and we may be interested in joining them once specifics become clear.

- NTT is globally top 5 both in network and IT service with 2.5B USD R&D spending. We are one of the three companies that are top 3 in all of US, Europe and Asia in Internet backbone. According to a third party analysis, we carry over 30% of global Internet traffic. In security, NTT has over 3,000 security professionals and more than 10 SOCs.
- In the US, NTT has 7B USD revenue and 42,000 employees. We provide a wide variety of service offerings in the US such as advisory services, digital and application services, infrastructure, cloud, security as well as BPO.
- As our testimony to commitments to participate public-private initiatives in the US, we have been participating in CSCC, CSRIC, ACT-IAC Blockchain working group, Illinois Blockchain Task Force, Virginia Governor Elect's Technology Policy Council etc.

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
Otemachi First Square East Tower 1-5-1 Otemachi, Chiyoda-ku, Tokyo 100-8116 Japan

- We are willing to participate in information sharing among ISPs (Action 2.1) and Information sharing standardization (Action 2.4). For example, in order to realize "Multi-DDoS mitigation service," which we mentioned above, we are starting to discuss technical challenges and operational ones with some major ISPs in the US.
- We are also willing to participate in Innovative R&D for prevention and mitigation of distributed threats (Action 1.3). We have 12 R&D laboratories in Japan and more than 2,000 research engineers are working. We cover a variety of R&D topics such as quantum computing, AI, IoT, Security, network technologies, applications and so on (http://www.ntt.co.jp/globalRD/). Secure Platform Laboratories, one of our laboratories in Tokyo, has over 200 security experts and takes a lead in innovative security R&D. We would like to continue to discuss the possibility of R&D collaboration with some enterprises and research institutions in the US.
- Since we provide network and software development services to corporations and government (both Federal and States), Secure software development (Action 1.2), Efficient network security (Action 3.1), Network architecture design (Action 3.3) may have relevancy to our capability. We may be interested in participating in them once specifics become clear.