NTT

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

July 21, 2017

Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

NTT appreciates the opportunity to submit comments to NTIA on this important challenge.

Our comments, described in the attachment, are based on our commitments to contribute to building global cyber resiliency. We welcome the opportunity to answer any questions regarding this document and thank you for this opportunity.

Sincerely Yours,

Shinichi Yokohama
Head, Cybersecurity Integration
NTT Corporation

Attachment

Introduction

Botnet is an eco-system problem which requires a whole eco-system approach.
It is also an international problem which requires global collaboration.

NTT provides IP backbone service across the world.
According to a third party analysis, there are three ISP's that rank top five in all of the three region, i.e. US, Europe and Asia. NTT is one of them.
With such scope and scale as a global Tier 1 provider, we have been observing threats in the Internet over a decade. In 2016, we observed two key trends that are relevant to botnets.

Ultra-scaling of DDoS

Between 2007 and 2012, the largest DDoS size was double-digits Gbps. For example, in 2012, 55Gbps was the largest DDoS attack of the year. Since then, the size has increased significantly. In 2016, the largest DDoS was 1.2 Tbps which is more than twenty 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, according to Arbor analysis.

Asia generates IoT attacks

Our Global Threat Intelligence Center 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 this high volume of attacks coming from devices in Asia is that the products in Asian market have historically been vulnerable to compromises and subsequent reuse in attacks.

With exponential increase of both scale and frequency of large size DDoS attacks, it is our belief that collaboration among all eco-system players across national boarder, including Asia, is indispensable for enhancing society-wide ability to reduce botnet threats. For example, Tokyo is going to host Olympics/Paralympics 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 following sections describe what NTT does today and what we propose from three angles, i.e. Technical Solution, Operational Solution, and Legal Solution.

Technical Solution

What we do today

Against DDoS, NTT has accumulated a rich set of data about DDoS attack patterns. Based on our analysis of such attack pattern data, we have developed proprietary DDoS mitigation capabilities. DDOS mitigation services to our clients are provided by combining these proprietary capabilities and 3rd part equipment vendor capabilities.

NTT also has developed proprietary SIEM (Security Information and Event Management) engine. Our analysis shows NTT's SIEM has low false positive detection. We protect both ourselves and our clients by Managed Security Services enabled by SIEM engine and high skill analysts.

Foundation to these DDoS mitigation and SIEM engine are our research efforts. We have proprietary honeypots and conduct malware analysis with global scale by laboratories and advanced analysts at SOC (Security Operation Center)'s. We are also working on developing botnet detection capabilities based on DNS analysis etc.

What we propose as collaboration

Based on above mentioned experience and on-going works, we propose below as a potential joint effort among stakeholders. Automation of detection and responses will be a key for enabling effective counter measures.

- Multi-DDOS mitigation services: If service providers collaborate across individual infrastructures so that their DDoS mitigation services, which are currently provided independently, are synchronized and orchestrated, we will be able to push malicious traffic closer to the source. NTT plans to launch Software defined Multi-DDOS mitigation services by making API available to cloud-based DDoS mitigation providers. Also, NTT is discussing with major carriers to jointly collaborate on DDoS mitigation
- Botnet infrastructure detection: If network providers, vendors, and others like law enforcements co-work by sharing information and analytic work, we will be able to detect bot masters and their infrastructures more effectively.

Operational Solution

What we do today

In Asia, not many ISP's have DDoS mitigation capabilities by themselves. For example, in Japan only four ISP's have such capabilities. In ASEAN countries, typically only one provider in a country has such capabilities. As a Tier 1 service provider that has strong foot prints in Asia, NTT provides mitigation services to other ISP's.

In Japan, industry and government have undertaken botnets take-down initiatives in the past. Cyber Clean Center is one example. Between 2006 and 2011, Telecom-ISAC (currently ICT-ISAC and of which NTT is a member), and JPCERT/CC, with financial support from the government, co-worked with security vendors to identify botnet infected users and provided clean-up tools to the infected users. 76 ISP's participated to this initiative and level of infected traffic was reduced from 2.5% to 0.6%. ICT-ISAC continues similar activities with its working groups.

Globally, NTT actively participates to threat information sharing including those around botnets. We do so as a member of FIRST and NCFTA.

What we propose as collaboration

Based on above mentioned experience and on-going works, we propose below as a potential joint effort among stakeholders.

- Botnet take-down initiative with international collaboration: If an initiative like Cyber Clean Center is done through international collaboration, our systematic capabilities to reduce botnet threats will be significantly enhanced. It is realistic that we start from a few countries, as opposed to many, since coordination efforts required will be not negligible.
- Mutual support between major ISP's: Major ISP's have different geographic presence in their infrastructures. If two ISP's have geographically complemental infrastructures, mutual support agreements between these two will make sense.
- Vulnerability management in installed end user devices: If network service providers are to contribute to managing vulnerabilities in end user devices that are already installed, collaboration with device manufacturers and sellers is indispensable. In fall 2016, when Mirai malware infected home routers in some European countries, service provider and device manufacturer collaborated and provided patches on-line.

- Financial incentives: Participants to collaborative operations contribute to keeping a social infrastructure clean and reliable. However, return from such efforts is not directly linked to individual contribution. It is desirable if some financial supports or incentives are provided to participating players.

Legal Solution

What we do today

In Japan, within current legal framework, NTT takes actions to protect customers and network service from botnets and malicious communications. One type of such action is legitimate self-defense. We shut down communication from malicious traffic sources, if such traffic is causing troubles for us to full fill our mission as a service provider. Another type is client service. We monitor, warn and shut down malicious traffic, as a security service to clients. In doing so, we obtain prior consent from the clients.

Key issues to be considered

Each country has its own legal framework, and service providers comply with such statutory requirements. Since botnets threats are international and across the borders, international harmonization of legal frameworks to enable speedy and early stage actions will be needed. Below is an example of issues to be considered for international legal harmonization.

- Monitoring and detection

  Conditions to monitor: Are service providers allowed to monitor always? If not, under what situations? For what purposes?

  Type of information: What specific information are service providers allowed to obtain? IP address, port number, protocol number, packet inspection, etc.

  Methods: Where within network do service providers monitor, with what technology?
- Information sharing with other network service providers

  How to protect or minimize adversary effects, such as causing unintended attacks?

  How to ensure protection of privacy, trade secret, etc?
- Traffic mitigation

  Under what conditions are service providers allowed to execute mitigation actions?

  What, if any, reporting to authority is needed?
- Vulnerability of devices

  How to ensure vulnerable devices are not sold in the market?

  How to ensure vulnerable devices are not connected to the network?

  How to make users aware that their devices are vulnerable and connected to the network?

Once these legal issues are harmonized, a collaborative effort becomes possible and the risk of global botnet attacks will be reduced.

Closing

Given the multi-dimensional nature of botnets challenges, some of our comments are overlapped and interlinked, but such overlap and interlink testifies the importance of collaboration across multiple stakeholders. We do not think what we describe in above sections are complete solutions. They should be positioned as inputs from a view point of one of the players. It is our hope that our comments contribute to the development and design of broader collaborative efforts and work streams that will be undertaken in coming multiple years. NTT is willing to be a part of such efforts and to participate to work streams wherever we can make positive, significant and lasting contribution.