

ITU Botnet Mitigation Toolkit and Pilot Field Project

ITU Regional Cybersecurity Forum and
Seminar on the Economics of Cybersecurity

Brisbane, Australia

15 July 2008

Suresh Ramasubramanian

<cybmail@itu.int>

ICT Applications and Cybersecurity Division
Policies and Strategies Department, BDT
International Telecommunication Union

.....

General Principles of The Toolkit

- This concept is based on several previous cybersecurity initiatives, not necessarily botnet focused. For example the OECD Anti Spam Toolkit.
 - Multistakeholder, Multipronged initiatives required, No Silver Bullet ..
 - Yes, these are clichés, but they're still true.
 - Technical measures alone wont be enough, nor will laws.
- This toolkit will be based on:
 - The context of a larger cybersecurity readiness strategy
 - Top down and bottom up public private partnership between government , industry, technical community, civil society working in ICT4D / Access and other relevant stakeholders.
 - Optimum use of existing initiatives and structures

Original Inspiration : Australian Internet Security Initiative (AISI)

- Australian Communications and Media Authority initiative
 - In partnership with 25 Australian ISPs
 - ACMA collects data on IPs emitting malware
 - Identifies IPs operated by participating Australian ISPs
 - Notifies ISP responsible for affected IPs
 - ISPs undertake to mitigate malware activity from infected IPs
 - Notify infected customers
 - Change security and filtering policies as necessary
- AISI project working internationally to fight botnets
- ACMA has agreed to assist ITU project and extend AISI to other ITU Member States

ITU Botnet Mitigation Package

- Identify coordination agency for a nationwide botnet mitigation strategy
 - Multi-stakeholder, Multi-pronged Approach (like OECD spam toolkit)
 - Public-Private Partnership
 - Coordination of local and global efforts
 - Make best possible use of existing initiatives and structures
- Infrastructure for botnet scanning, measurement and mitigation
 - Capacity building on tools and techniques to track botnets
 - Identification of trusted interlocutors (e.g., international security and AV research community, CERT teams) for incident reporting
 - Reports feed into a national instance of the AISI system
 - ISPs volunteer to mitigate incidents reported on their network
 - Alerts may be sent by a government regulator or CERT, nationwide

ITU Botnet Mitigation Package

- Detection and takedown of botnet hosts and related infrastructure
 - Automation using walled gardens and other methods
 - MAAWG best practice on walled gardens -
[www.maawg.org/about/whitepapers/MAAWG Walled Garden BP 2007-09.pdf](http://www.maawg.org/about/whitepapers/MAAWG_Walled_Garden_BP_2007-09.pdf)
 - Reported incidents may be malware infected PCs, botnet “command and control” hosts, domains registered for use by botnets, payment gateways used to process payments for products advertised using botnet spam ..
- Building awareness of security best practices for ISPs, e-commerce sites
- Promotion of Internet safety awareness among the general public
 - Engagement with the technical (network operations, anti phishing etc) community and civil society
 - Ensuring grassroots penetration of training initiatives

ITU Botnet Mitigation Package

- Framework for national botnet related policy, regulation and enforcement
- Multi-stakeholder international cooperation and outreach
 - Phase 1 (2007):
 - Downloadable toolkit/guidelines for ITU Member States
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
 - Phase 2 (2008/2009):
 - Targeted national/regional assistance initiatives
 - First pilot in Malaysia
 - Cooperation with other partners
 - LAP, APEC-TEL/OECD, Interpol, and industry / technical community / civil society groups (MAAWG, APWG, FIRST, NSP-SEC, Spamhaus, RIRs, ISOC..)

Malaysia Pilot - Overview

- Facilitated by the Malaysian Communications and Multimedia Commission (MCMC)
- A practical application of the concepts and suggested best practices mentioned in the ITU Botnet Mitigation Toolkit
 - Best practices from policy, technical and civil society / ICT groups selected and implemented, their results observed, feedback collected.
 - What worked? What didn't work? What modifications were required to currently accepted best practices to make them work together?

AISI Malaysia Pilot

- Implement AISI in Malaysia
 - Source feeds from various sources
 - Anti-malware / antispam groups, CERTs, Honeypot networks ...
 - Preferably in the RFC standardized IODEF format
 - Extend to (say) two ISPs as an initial pilot
 - ISPs agree and volunteer to receive these reports
 - And to mitigate abuse on their networks based on these reports
 - ISPs contribute and update their ASNs / IP address space that they wish to receive alerts for
 - Then implement at other ISPs over the course of the pilot and afterwards

Workshops

- Policy and Technical workshops
 - Policy workshops focused on government (regulators, law enforcement, judiciary) personnel
 - Technical workshops focused on “in the trenches” mitigation by ISPs and Industry
- Workshop material made available for future education initiatives
 - Translated into the UN official languages
 - Additionally, the MAAWG best practice documents are currently being translated into the UN official languages

Technical Workshops

- Workshop for ISPs / NSPs
 - Instructors from Cisco / NSP-SEC
 - Hosted at Universiti Sains Malaysia, Penang
- Workshop for banks & ecommerce sites
 - Facilitated by APWG
 - Two workshops, one high level, for senior management and another with hands on operational content
 - instructors from Wachovia Bank (TBC)

Policy Workshops

- A series of policy focused workshops
 - Focused on different government departments and their needs
 - Regulators, Law Enforcement Agencies, Prosecutors, Judiciary ...
- Workshops and briefing sessions on the sidelines of an international conference on cybersecurity and botnets, to be hosted jointly by ITU and MCMC (tbc).

Feedback and Participation

- ITU welcomes comments on the Botnet Mitigation Toolkit and the pilot project
- ITU would also appreciate insights into similar field testing of best practices, especially in emerging economies, if available
- Offers of assistance (such as providing reporting feeds, workshop instructors or anything else) are welcome.
- Project email address : cybmail@itu.int

More Information

- ITU-D ICT Applications and Cybersecurity Division
 - www.itu.int/ITU-D/cyb/
- ITU Botnet Project Website
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
- Botnet Mitigation Toolkit Overview
 - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf
- Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
 - www.itu.int/ITU-D/cyb/events/
- Cybersecurity Publications
 - www.itu.int/ITU-D/cyb/publications/

International Telecommunication Union

Committed to Connecting the World