General Principles for a Botnet Mitigation Toolkit

Suresh Ramasubramanian
suresh@hserus.net
http://www.hserus.net

Botnets – An Overview

- What is a Botnet?
  - A collection of infected and compromised computing devices, harnessed together and remotely controlled for malicious purposes
- How powerful is a Botnet?
  - Supercomputers
  - Distributed Computing Systems
    - BOINC – Used for SETI@Home, Atomic Physics
    - People agree to donate spare computing resources
  - Botnets: A special case of Distributed Computing
    - Without the consent of the computers' owners
    - More computing power than a supercomputer – for free

The Botnet Economy

- Virus Writers, Botherders, Clients
  - Virus writer writes malware, infects computers to create a botnet
  - Botherder operates the botnet's "command and control" (C&C)
  - Clients hire botnets to use for Spam, DDoS, Identity Theft
- Highly developed underground economy
  - Underground channels of communication
    - "Secret" forums and chat rooms that frequently shift location
    - Access shared on a need to know basis, new entrants may need to be vouched for by an existing participant
  - Botherders offer support contracts to clients
    - Guaranteed replacement of botnet in case antivirus researchers release a fix for the malware, or the botnet is taken down
- Organized crime involved in all stages of the economy
  - Employ virus writers to create malware
  - Carry out spam campaigns, espionage, ID theft, cyber attacks
  - Launder money stolen from victims

Evolution of Botnets

- C&C centers harder to trace
  - Originally hosted on public IRC channels
  - Now encrypted, access restricted C&C software
- C&C centers may be hosted on botnets
  - Increased redundancy
  - Makes takedown harder
- New “headless” single use botnets
  - No centralized control or C&C required
  - Instructions embedded into the malware
  - New malware and botnet created for a new task
  - Cannot stop botnet by taking down its C&C

What can you do with a botnet?

- Spam
  - The most visible use of botnets
  - Botnets can host an entire spam campaign
    - DNS servers, website hosting, spam sending
    - Content can change location from PC to PC, country to country, in minutes
  - “Take” from a spam run can be reused
    - 419 scam artists now buying lists of compromised accounts from botherders, using these to spam
  - Spam is just the tip of the iceberg.

What else can you do with a botnet?

- Attack a country's Internet infrastructure
  - Estonia – 128 unique DDoS attacks in two weeks
- Extortion
  - Threaten to DDoS and cripple ecommerce websites
- Identity theft and Industrial Espionage
  - Steal credit cards, passwords etc from infected PCs
  - Use the computing power of a botnet to break into secured networks and steal data, credit cards
- Stock "Pump and Dump" scams
  - Use spam from botnet PCs to advertise a stock
  - Trade in this stock using online share trading accounts from infected PCs, artificially boost prices

Approaches to Botnet Mitigation

- Several such approaches exist, but not botnet focused – eg: OECD Spam Toolkit
- Multistakeholder, Multipronged initiatives required, No Silver Bullet, etc etc
  - Yes, these are cliches, but they're true nonetheless. Technical measures alone wont be enough, nor will laws.
- A government must identify a nodal agency for a nationwide botnet mitigation strategy
  - It should be based on top down and bottom up public private partnership (not just government+ vendors / contractors, multiple groups from the technical community – CERTs, ccTLDs ISPs and Network Operators, as well as NGOs doing work in ICT4D / Access, etc.
  - Make best possible use of existing initiatives and structures. Don't reinvent wheels.
- Infrastructure for botnet scanning, measurement and mitigation
  - Training and deployment on tools and techniques to track botnets (darknets, honeynets, passive DNS analysis etc)
  - Identification of trusted reporters (international security and AV research community, CERT teams et al) for incident reporting
  - ISPs commit to take action on reported incidents. This may require voluntary commitment from the ISPs, or in some economies it may require that alerts be sent by (say) a regulator or government CERT agency.

Approaches: Continued

- Detection and Takedown of botnet hosts and infrastructure
  - Infected PCs (automate as far as possible), C&C hosts, domains registered for a botnet, payment gateways used by botnets etc need to be taken down or where required, made available for forensic analysis required for investigation
- Awareness of security best practices for ISPs, ecommerce sites
  - Workshops organized by NSP-SEC, APWG and other industry / technical groups
- Ensure public access to secure ICT, awareness of Internet safety
  - Engage local civil society for assistance and grassroots penetration
  - Make sure that initiatives distributing computing resources to underprivileged people provide secure computing resources and internet access
- Nationwide framework for botnet related policy, regulation and enforcement;
  - This has to be put in a broader context of a country's legal and regulatory systems, critical internet infrastructure protection (CIIP) mechanisms, industry and public awareness etc
- Multistakeholder international cooperation and outreach
  - COE Cybercrime Convention, LAP, APECTEL/OECD, MAAWG, APWG, NSP-SEC ,FIRST, APCERT, APTLD etc etc
  - There are several such groups actively or peripherally involved in this effort – they need to work together, to at least coordinate their related efforts

Common Policy Shortcomings

- Lack of relevant Cybercrime and antispam legislation
  - Existing Cybercrime / spam laws may need to be updated or revised, keeping botnet related crime in mind
- Capacity building for regulators, police, judiciary
  - Training existing officials may be supplemented by co-opting or active recruitment of technical experts
- Paucity of international cooperation and outreach
  - Participation in local, regional and international initiatives
  - Engagement of relevant government, regulators, law enforcement with their peers and other stakeholders around the world
  - Active outreach to countries and stakeholders known to be particularly susceptible to Cybercrime issues

Industry / Civil Society Shortcomings

- ISPs, eCommerce vendors require capacity building
  - Engagement with international industry groups
  - Promotion of industry wide security best current practices
    - Antispam, Anti Malware, Credit Card Fraud, Network Security
  - Suggested re-engineering of security policies
- Education and access to secure ICT for users
  - Awareness of common scams
  - Availability and use of firewalls, Antivirus Software
  - Motivation to avoid the use of pirated software
- Paucity of cooperation and public private partnerships
  - Participation at grassroots, national and international levels
    - Participation has to be relevant, meaningful and informed.
    - Capacity building [and funding] for relevant stakeholders to ensure meaningful participation in local, regional and international initiatives
    - Bridge the information and perception gaps between stakeholders

Suggested practical activities for a nationwide botnet mitigation effort

- Measures for botnet detection, measurement and mitigation
- Identify existing initiatives, best practices and stakeholders
  - Adapt existing best practices to suit local conditions, as necessary
- Organize workshops and on the job training relevant to botnets for Government, ISPs, Banking / eCommerce Providers etc.
  - Reach out to schools, cybercafés etc for public education campaigns.
- Build watch, warning and incident response systems
  - Nationwide alert system (CERT etc) to aggregate various public / semi private malware feeds (such as Team Cymru, Shadowserver etc), alerts from CERT and security research groups etc
  - Work with ISPs to implement mitigation procedures for these alerts
- Maintain open and public channels of communication
- Integrate botnet mitigation with general ICT development
  - Pandemic treatment and mitigation on the lines of public health initiatives against SARS or Avian flu.
  - Holistic approach required to improve the general “Internet Health”

Thank you

I regret that I was not able to come to Taipei due to family commitments.

Please feel free to email me any questions that you have, at suresh@hserus.net