ITU Botnet Mitigation Project: Background & Approach

September 2007

Suresh Ramasubramanian & Robert Shaw
<cybmail@itu.int>

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

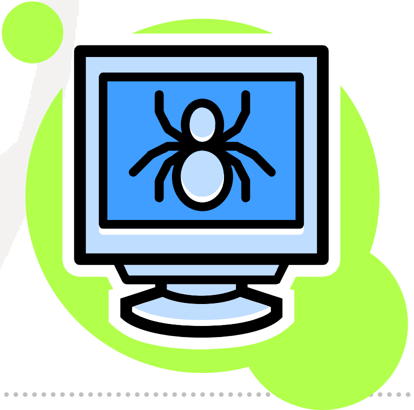
Botnets – An Overview

- 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?
  - Like supercomputers created through distributed computing systems
    - e.g., BOINC: used for SETI@Home, Atomic Physics
    - People agree to donate spare computing resources
  - Botnets: a special case of distributed computing
    - Without consent of computer owner (a zombie)
    - Hijacking of computing resources

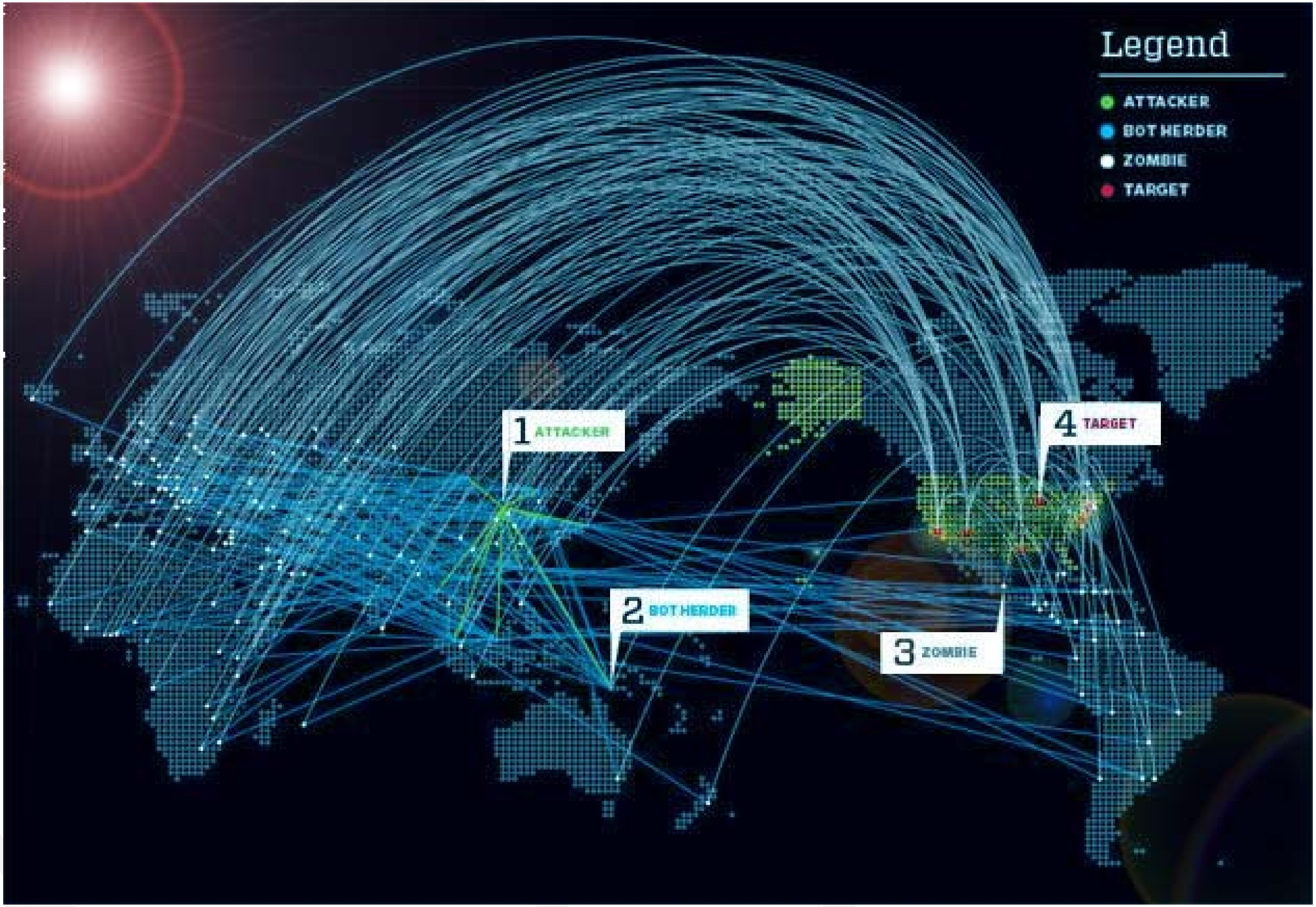
Botnets – An Overview cont’d

- Botnets are a worldwide menace, widely used by spammers and cyber criminals
- Use of botnets for cybercrime has increased and become more refined since 2002-3 when first mass mailer worms such as Sobig and Sober were released



Latest Generation

- 2007 generation botnets such as Zhelatin (Storm Worm) are particularly aggressive using advanced techniques such as fast-flux networks to make it harder to shut down and even striking back with denial of service (DDOS) attacks against security researchers or vendors trying to mitigate the botnet
  - *"Fast-flux service networks are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. These constantly changing architectures make it much more difficult to track down criminal activities and shut down their operations."*
    - Honeynet Project & Research Alliance



Source: Wired Magazine

The Botnet Ecosystem

- Virus Writers, Botherders, Clients
  - Virus writer writes malware, infects computers to create botnet
  - Botherder operates the botnet “command and control” (C&C)
  - Clients hire botnets to distribute spam, launch Distributed Denial of Service (DDoS) attacks, to conduct identity theft
- Highly developed underground channels of communication
  - “Secret” forums/chat rooms that shift location
  - Access on a need to know basis, new entrants may need to be vouched for by existing participant

The Botnet Ecosystem cont‘d

- Botherders now offer “service level agreements” to clients
  - Guaranteed replacement of botnet in case anti-virus researchers release fix for malware or botnet is taken down
- Organized crime involved in all stages of ecosystem
  - Employ virus writers to create malware
  - Carry out spam campaigns, espionage, ID theft, cyber-attacks
  - Laundering of money stolen from victims

Evolution of Botnets

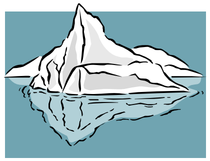
- C&C centers harder to trace
  - Originally hosted on public IRC channels
  - Now encrypted, access restricted C&C software
- C&C centers may be hosted on botnets
  - Increased redundancy
  - Makes takedown harder
- New “headless” single use botnets
  - No centralized control or C&C required
    - new generation of P2P botnets
  - Instructions embedded into malware
  - New malware and botnet created for a new task
  - Cannot stop botnet by taking down its C&C

Evolution of Malware

- Self-propagating: infected hosts infect other hosts
  - Infection vectors include email, P2P networks, open shared network folders, Skype, visiting infected website
  - Newer malware spreads faster than older generations
- Spread resembles global pandemic (SARS, Bird Flu)
  - Can similar threat models/mitigation mechanism theories be applied?
- Analysis, Detection and Removal more difficult
  - Self-destruct mechanisms to destroy data if malware removed
  - "Droppers" malware download more payload onto compromised host
  - Encryption and debuggers / Virtual Machine (VM) traps to prevent forensic analysis

What can you do with a Botnet?

- Send spam
  - Most visible use of botnets
  - Botnets can host entire spam campaign
    - Including 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
  - But 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/Blackmail
  - Threaten to DDoS/cripple e-commerce websites
- Identity theft and Industrial Espionage
  - Steal credit cards, passwords, etc. from infected PCs
  - Use 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 stock
  - Trade in this stock using online share trading accounts from infected PCs, artificially boost prices

ITU Botnet Mitigation Project originally inspired by Australian Internet Security Initiative (AISI)

- Australian Communications and Media Authority (ACMA) 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 on their networks
    - Notify infected customers
    - Change security and filtering policies as necessary
- AISI project working internationally to fight botnets and 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
  - 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 interlocuters (e.g., international security and AV research community, CERT teams) for incident reporting

ITU Botnet Mitigation Package

- Detection and takedown of botnet hosts and related infrastructure
  - Infected PCs (automate as far as possible), C&C hosts, domains registered for botnet, payment gateways used by botnets, etc
- Build awareness of security best practices for ISPs, e-commerce sites
- Promote general Internet safety through end-user awareness programmes, engagement of civil society for assistance and grassroots penetration

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
  - Phase 2 (2008/2009): Targeted national/regional assistance initiatives
    - Discussions with Malaysia, India
  - Cooperation with other partners?
    - LAP, APEC-TEL/OECD, MAAWG, APWG, Interpol?

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

Helping the World Communicate