Botnets: Measurement, Detection, Disinfection and Defence

Dr Giles Hogben
ENISA
Overview

• Recommendations
  – Measurement and detection
  – Countermeasures
    • Threat picture
    • Roles, responsibilities and incentives
  – Focus on legal issues, information sharing
MEASUREMENT AND DETECTION
The need to assess the threat level

• Deciding on investments (100’s of millions of Euros): in security measures. For governments as well as for businesses.

• Defining the political agenda: Botnets are a major threat to society to be engaged on governmental level.

• Assessing the success of measures: how do we know a technique worked
A quarter of US PCs infected with malware: OECD

June 2, 2009

One in ten websites 'is infected with malware'

Jonathan Richards

ZDNet

Report: 48% of 22 million scanned computers infected with malware

By Dancho Danchev | January 27, 2010, 1:42pm PST
Measurement and Detection

• Problems identified with current measures
  – Lack of accuracy
  – Transparency of methodology
  – Incentives for exaggeration
  – Size is not everything
Size is not everything

- From Panda Labs: order of 500 computers (not a botnet but some characteristics in common) took down Visa.com during the Anonymous attacks
- But nobody ever quotes anything else
Impact depends on stakeholders

- Governments care about targeted theft of classified information and political/military targets.
- Financial organisations care about financial fraud and DDoS.
- Email services care about spam volume.
- E-commerce providers care about DDoS attacks.
Better impact indicators

- Distribution (origin)
- Spam statistics
- Bandwidth of attacks
- Data types harvested
- Financial damage
- Malware characteristics
KEY RECOMMENDATIONS FOR COUNTERMEASURES
Goal: Minimize botnet threat

Direction

Mitigate existing botnets
- Reduce number of infected systems
- Fight C&C infrastructure

Prevent new infections
- Slow down botnet spreading through early detection
- Protect systems
  - User awareness

Minimize profitability of botnets
- Increase security awareness
- Attack botnet value creation chain

Approach

Preconditions

- Reliable method for the detection of infections
- Analysis of C&C infrastructures
- Analysis of structures and patterns
- Identification of vulnerabilities
- Identification of primary assets of criminal value creation chain

Auxiliaries

- Information sharing, tracking of botnets
- Identification of C&C and comm. patterns
- Exploit discovery and information sharing
- Information campaigns and security education
- Derive botnet functionality and economics

Auxiliaries

- Host
  - anti-MW software
- Network
  - ISPs
- Takedown of C&C and arrest of botmasters
- Application of preventive measures
- Responsible operation, patching of systems
- Active support of users
- Improve anti-fraud, prosecute botmasters, create deterrence

Actions
Mitigate Existing Botnets

Mitigate existing botnets

- Reduce number of infected systems
- Fight C&C infrastructure
- Reliable method for the detection of infections
- Analysis of C&C infrastructures
- Host-level anti-MW software
- Netw.-level ISPs
- Information sharing, tracking of botnets
- Cleaning of systems
- Takedown of C&C and arrest of botmasters
Prevent new infections

- Slow down botnet spreading through early detection
- Protect systems
  - User awareness
- Analysis of structures and patterns
- Identification of vulnerabilities
- Identification of C&C and comm. patterns
- Exploit discovery and information sharing
- Application of preventive measures
- Responsible operation, patching of systems
Minimize profitability of botnets

Increase security awareness
Attack botnet value creation chain

Identification of primary assets of criminal value creation chain

Information campaigns and security education
Derive botnet functionality and economics

Active support of users
Improve anti-fraud and prosecute botmasters
Responsibilities

Governments
- Define clear and consistent laws
- Prosecute criminals
- Define capabilities
- Define central contact points
- Data protection

End-users
- Keep machines clean
- Civic responsibility
- Corporate social responsibility

ISPs
- Identify, notify customers
- Help users clean machines
- Filter malicious traffic
- Detection, measurement
- Data protection

Software/OS Developers
- Write secure software
- Fix vulnerabilities (quickly)
- Detect attacks and inform users

Researchers/AV Vendors
- Detection
- Disinfection
- Responsible disclosure
- Malware analysis

Cybercriminals
- ... (not listed)

Victims
- Resist extortion
- Pursue perpetrators
Current incentives

- Beneficiaries: Cybercriminals
- Innocent bystander/unwilling participant: ISP, End-user
- Victims: eCommerce, Banks, Web 2.0, Advertisers, Governments
Rebalancing the incentives

**Government**
- Public private partnerships

**End-users**
- Bot-Frei
- Awareness raising
- Raise sense of social responsibility

**Software Vendors**
- Secure dev programmes
- SSE initiatives

**AV/Researchers**
- Fast legal procedures
- Reward for reporting
- Clarify capabilities
- Information sharing

**ISP’s**
- Financial incentives for end user cleaning initiatives
- Clarify and harmonise DP laws

**Criminals**
- Prosecute and arrest
- Attack all parts of value-chain—esp those with no backup—e.g. money-laundering.
- Attack revenue streams

**Victims**
- Mutual assistance—e.g. in legal and other resources (Digital Addio-Pizzo)

**Incentives**
Information sharing

• Benefits
  – Coordination
  – View on trends
  – Faster reaction

• Challenges
  – Abuse report formats
  – Mutually beneficial sharing
  – Trust between parties.
  – Confidentiality - how to know when 2 teams are infiltrating the same botnet without alerting the botmaster?
Legal and Jurisdictional challenges

• Clear definition of who can do what in the EU 27 and beyond.
  – E.g. Status of IP address as Private Data
• Roles and responsibilities – points of contact across border – vide ENISA exercise.
• Empower people who are in a position to do something and clarify what
  – e.g. define clearly what botbusters can and cannot do.
  – E.g. Good samaritan provisions.
  – Quick reaction by law enforcement and justice.
  – Accelerated procedures – time is premium
• Find practical balance between DP laws and system security.
Legal Report

• Work in progress: separate report on legal issues Q2 based on survey of experts at EU and MS level.
• Stakeholder capabilities e.g. Packet inspection, Takedown, Remote disinfection
• Emergency powers
• Liability of stakeholders (for damages, non-action, disclosure)
• Gaps and recommendations
Key messages

• We don’t have good enough information on threat levels.
• Provide the right incentives to those in a position to fight botnets.
• Efficient and comprehensive international co-operation
• Clarify and harmonise legislation
Questions?


• Botnets: 10 hard questions – Analysis by ENISA and expert group. [http://www.enisa.europa.eu/botnets-10Q](http://www.enisa.europa.eu/botnets-10Q)

• Legal analysis and recommendations. In preparation
Group Composition

- National and pan European Internet Service Providers: 3
- Antivirus Software Developers and Security Solutions Providers: 21
- Operating System Providers: 4
- Application and Network Providers and Developers: 2
- Web 2.0 and Social Network Site Providers: 1
- Academia: 4
- CERTs: 14
- Online User Communities and Consumer Protection Associations: 3
- Regulators and Policy Makers: 7
- Law Enforcement Agencies: 3
- Pan European Associations of Providers: 4