Towards Incentivizing ISPs To Mitigate Botnets

Qasim Lone
Giovane C. M. Moura
Michel van Eeten
{Q.B.Lone,G.C.MoreiraMoura,M.J.G.vanEeten}@tudelft.nl

Faculty of Technology, Policy, and Management
Delft University of Technology

Autonomous Infrastructure, Management and Security
(AIMS 2014)
Brno, Czech Republic
June 30, 2014

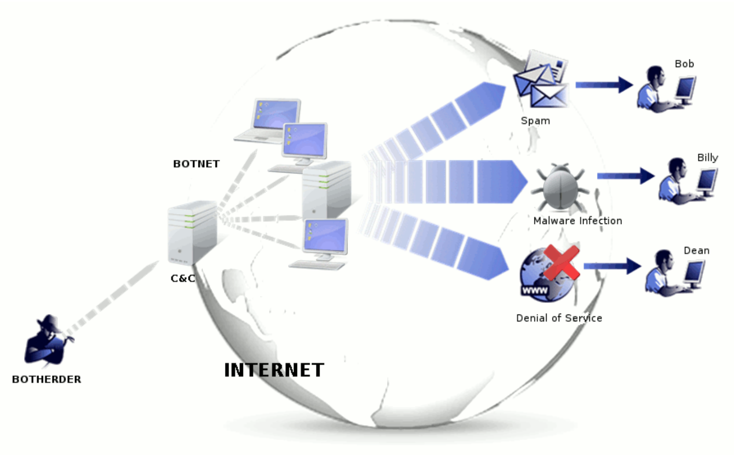
TU Delft Delft University of Technology

Overview

Outline

- Botnet overview
- Role of ISPs
- Research problem
- Next steps

What is botnet ?



Botnet Infrastructure

source:http://www.f-secure.com/en/web/labs_global/articles/about_botnets

Role of ISPs

- ISP form a centralized control point
- Malicious hosts are concentrated in a small number of ISPs
  - 50 ISPs account for around half of all spamming IP addresses
  - 20 Autonomous Systems (AS), out of 42,201, were responsible for 50% of all spamming IP addresses

Why compare ISPs ?

- Limited incentives for ISPs to invest in botnet mitigation
  - ISPs investing in mitigation will suffer from higher cost of notification then their competitor
  - Users and stakeholder can not differentiate between good performing from bad ones
- Comparable and relative metrics can quantify how “bad” an ISP is
- Publishing such numbers may incentivize them to clean it up

Research Problem

Research Questions

1. What kind of network measurement data is required to statistically account for botnet population in the networks of ISPs ?
2. How to turn the measurements into comparative relative metrics for ISPs performance in botnet mitigation ?
3. How can these metrics contribute to evaluate and incentivizing botnet mitigation by ISPs ?

RQ1: Data requirements to measure botnet population

Data Types

- Data collected outside of botnet for e.g. spam, DDoS traffic
  - Cover wide range of botnets
  - Captured data has high number of false positive and negatives
- Data obtained by taking over command and control center of botnet
  - High accuracy of captured data
  - However, data is limited and is not representative of botnet population
- Longitudinal and comparable data needs to be selected to correctly estimate botnet population

RQ 2:How to turn the measurements into comparative relative metrics

Requirements for creating botnet metrics

- Metrics are required to be :
  - Consistent over time, normalized for e.g. on size of ISPs, comparable accross ISPs and representative of botnet population
- Some of the challenges include:
  - DHCP Churn
  - NAT
  - Measurement of relative potency of botnet

How can we compare ISPs ? Is ISP A better than B ?

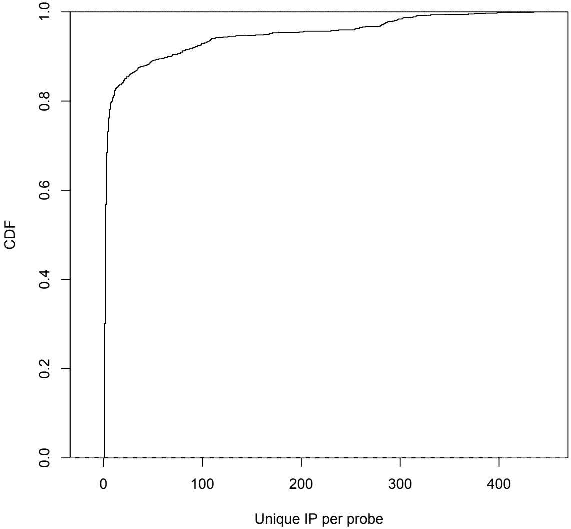
Challenges in creating botnet metrics

- **IP addresses $\neq$ botted IPs [1]**

Country	# IP addresses	# Bot IDs	DHCP Churn Factor
US	158,209	54,627	2.9
IT	383,077	46,508	8.24
DE	325,816	24,413	13.35
PL	44,117	6,365	6.93
ES	31,745	5,733	5.54
GR	45,809	5,402	8.48
UK	21,465	4,792	4.48
NL	4,073	2,331	1.75
Totals:	**1,247,642**	**182,800**	**6.83**

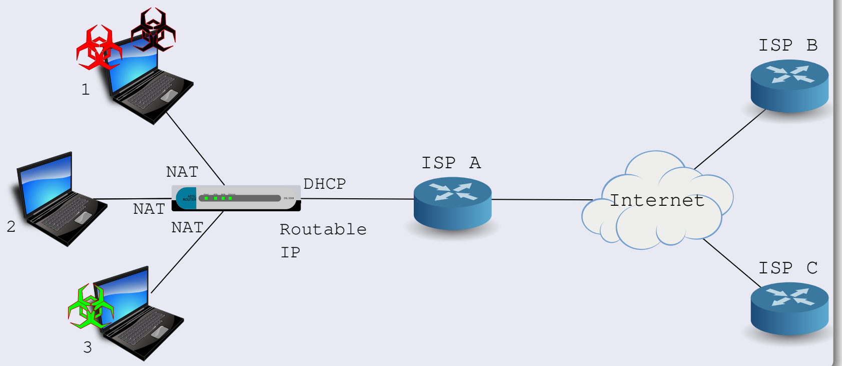
Top 10 infected countries by Torpig botnet (source: [2])

DHCP Churn – RIPE Atlas



Problems due to NAT

Releationship between ISPs, botnet and home users



How developed metrics can be used to maximize incentives ?

Publishing comparision of ISPs

1. Publish annual/quarterly/monthly reports
2. Automated website with live data
3. Comparisons which are easily understandable for majority of Internet users.

Next Steps

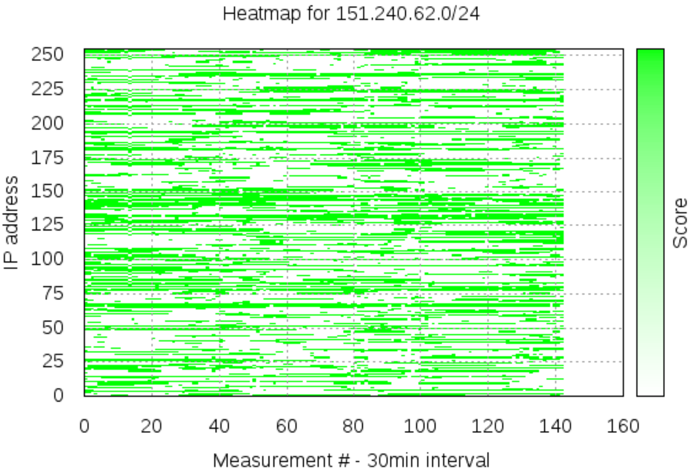
1. Active measurement approach to measure churn using ICMP
2. Analysis of data sources with different statistical properties
3. Normalize the count of infected machines using ISP size

References I

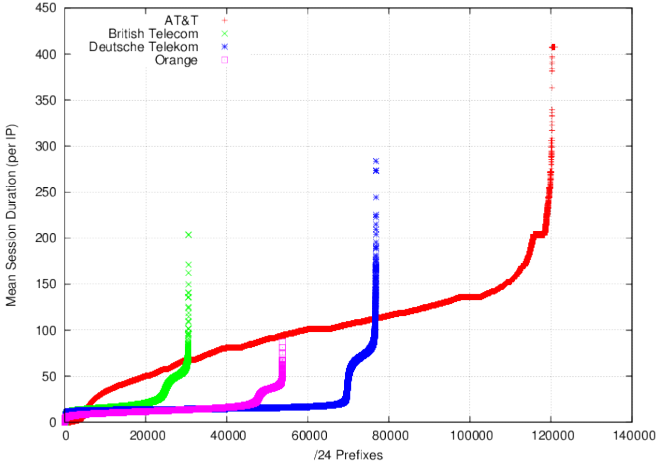
- M. A. R. J. Z. Fabian and M. A. Terzis, “My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging,” in *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets, Cambridge, USA*, 2007.

- B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, “Your botnet is my botnet: analysis of a botnet takeover,” in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 635–647, ACM, 2009.

Calculating Churn for an entire /24



Session Times


AT&T +
British Telecom ×
Deutsche Telekom ✳
Orange □
Mean Session Duration (per IP)
/24 Prefixes