M3AAWG
MESSAGING MALWARE MOBILE

The Bot Problem

Mike O'Reirdan, M3AAWG Co-Chairman
Ram Mohan, M3AAWG
29th October 2012
New Delhi

Panelists

- Suresh Ramasubramanian (IBM)
- Mike O'Reirdan (M^{3}AAWG / Comcast)

What will we look at?

M3AAWG
MESSAGING MALWARE MOBILE

- How do you see the problem?
- Focus on bots / malware and consumer challenges
- Policy is key
- Brief review of global efforts
- Monetization
- Technology
- Resources
- Role of registrars
- Next steps, reports by table

Why is M³AAWG focusing on bots in India?

Rank	Country	Infections
1	**India**	**1,536,013**
2	China	1,153,704
3	Vietnam	636,706
4	Brazil	557,280
5	Turkey	427,719

Source: CBL (http://cbl.abuseat.org/nas.html)

.IN is the 5th most abused TLD in the world

[Source: SURBL (http://www.surbl.org/tld)]

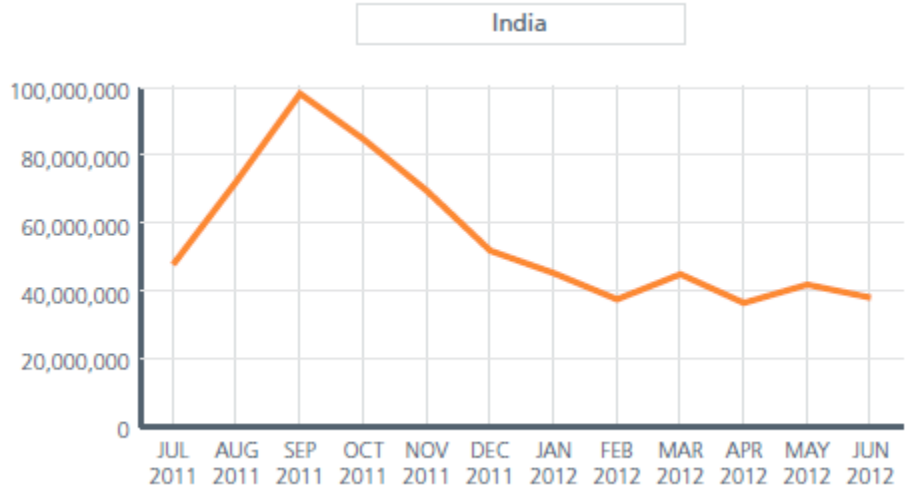
Indian ISPs among largest in global spam counts

M3AAWG
MESSAGING MALWARE MOBILE

Domain	Global Rank	Traffic	Spams/bot	% Infected
Sancharnet.in	3	782,484	1	11.665%
Airtel.in	7	146,920	0	3.674%
Tatatel.co.in	11	64,868	0	15.407%
Vsnl	17	586,026	6	1.355%

Source: CBL (http://cbl.abuseat.org/domain.html

Spam Counts - India



Source: McAfee (http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf)

Policy is key

- May sound like a list of roles but up to regulators and policy folks to work together to ensure everyone plays their position
- Not just the role of the ISP
- ISPs core competency
  - Detection and notification, manages relationship between IP resource and subscriber
- Other players
  - Law Enforcement
    - Prosecute and lock up cyber criminals
  - OS Vendors
    - Secure operating system
    - Regular patching
  - Tools vendors
    - Tools are often overwhelmed

Global efforts

- US
  - FCC Bot Code
    - ABCs for ISPs
  - Major programs at several ISPs
    - Century Link
    - AT&T
    - Comcast
    - Cox
- Germany / Eire
  - BotFrei.DE
  - Irish Anti Botnet Initiative
  - Spreading to 14 European countries
  - EU funded

Global efforts

- Finland
  - Interesting regulator led model
  - Carrot and stick; very carrot focused
- Australia
  - iCode since 2010
  - Australian Internet Security Initiative
  - Looking at first major revision; metrics are the aim
- Japan
  - Cyber Clean Centre
  - Founded 2006
  - Wealth of resources including major section in English

Monetization

- Need financial justifications
  - ROI may need to be sought
  - Reduced churn of subscribers
  - Reduced numbers of call centre contacts
  - Spam can consume expensive bandwidth resource
- Free versus paid
  - Important not to make this seem to be an upsell for additional services
  - Need a prominent “free” remediation path
  - Often too complex
- Do your own Geek Squad approach
  - Geek Squad, large-scale consumer tech support organization; counters in computer stores and in-home support
  - Some ISPs have set up fee-based remediation services

Technology

M3AAWG
MESSAGING MALWARE MOBILE

- DNS
  - Passive DNS detection
  - Limited to bots that use DNS
  - Requires specialized intelligence on C+Cs
  - Does not capture P2P botnets
- DPI
  - Very useful to detect range of bots via signatures
  - Allows identification of malware
  - End user privacy implications
  - Depends on country attitude to DPI
- NetFlow
  - Analysis of traffic flows
  - Good for detecting botnets but not malware

Role of domain name registrars

- India-based registrars have the strongest ability to respond and curtail bad registrations:
  - Directi is one of the largest Indian reseller-based registrars, with prior abuse experience
  - Net4India is the largest retail based registrars, with a well-developed validation method
  - Mitsu is one of the fast growing registrars, with some current abuse
- Largest abuse seems to come from automated, non-verified systems
- Domains are one of the raw materials for botnets

Resources

- IETF Guide to bot remediation
  - RFC 6561
- IETF Guide to a possible notification system
  - RFC 6108
- Free data sources
  - Team Cymru
  - Shadow Server
  - Arbor Networks
- Free A/V
  - Avira
  - AVG
  - Microsoft Security Essentials
- Other free tools
  - Malwarebytes
  - Spybot
  - Adaware

DNS Changer

M3AAWG
MESSAGING MALWARE MOBILE

- FBI Operation Ghost Click
- First discovered in 2007 by private researchers
- Rove Digital
- DNS servers in the US
- Initially thought to be 4 million users infected, turned out to be less but still substantial
- November 8th 2011, 7 arrests, servers and cash seized
- DNSs run by ISC from Nov 8th 2011 to June 9th 2012
- Need to remediate end users
- Interesting statistics
  - Do nothing ISP -40%
  - Active ISP -80%

Current Indian ISP anti-bot efforts

- What are the current Indian anti-bot efforts?
- Is this seen as a priority effort for the Indian ISPs?
- What are the next steps?