“Irresponsibility at Scale”
from a CERT point of view

Dr. Cristine Hoepers

cristine@cert.br

Computer Emergency Response Team Brazil - CERT.br
Brazilian Network Information Center - NIC.br
Brazilian Internet Steering Committee - CGI.br
Which problems are we talking about?

All those that are possible or amplified by the lack of best practices implementation by the various players, like:

- DDoS and DRDoS
- Spam

From the perspective of the ones that need to implement best practices
- There is no immediate benefit
- The effects of the attacks from their perspective are negligible

From the perspective of the ones being attacked
- almost nothing can be done to stop the attack
- the effects are big and complex to mitigate
But it is not only a network/ISP perspective problem.

Other sectors also need to be involved:

- **Software development**
  - in general developers think that security is an add-on
    - to be implemented by someone else
  - but it needs to be incorporated from design to deployment and maintenance

- **Standards communities**
  - standards are developed without security considerations
  - then they try to create security standards to try and patch the problems created by other standards
The best practices and security layers are being postponed

- BCP 38 (antispoofing), Botnet remediation (disinfection)
- End user awareness/education
  - the users should have a chance to understand the risks

Other times the sectors are stuck in a “chicken and the egg” dilemma

- DNSSEC adoption

- More security on the routing system
  - RPKI e S-BGP

- Improvements or alternatives to the current digital certificate system
  - the current trust model is broken
Any examples on how we could start to move forward?
Port 25 Management in Brazil

A multistakeholder effort to reduce direct delivery from end user networks (mainly from botnets)

• Port 25 management is a technical recommendation from MAAWG, OECD, FTC, and so on

• So, why we don’t all implement this on the Internet?
  – Real life is more complex: legal issues, consumer protection, regulatory dilemmas, risks of technical problems, costs of implementation, no clear definition of the benefits, etc

Caveat: Other angles of the spam problem are being worked in other multistakeholder subgroups

• e-mail marketing self-regulation, legislation proposals, technical recommendations, user awareness
Regular Meetings to Negotiate Port 25 Mgmt Adoption

- Coordinated by CGI.br – with technical coordination by CERT.br/NIC.br
- Initial players: Telcos, ISPs and Associations of these sectors, Anatel (Telecom regulator), the CGI.br representatives for these sectors
- Players identified in further meetings: Federal Prosecutor’s Office, Consumer Defense organizations and Ministry of Justice
- Agreed on a coordinated effort for adoption:
  - 1st: ISPs offering Message Submission services and changing at least 90% of their clients’ configuration
  - 2nd: Telcos blocking outbound port 25 traffic – residential/3G networks
- A formal implementation agreement was signed
  - CGI.br, NIC.br, Anatel, Telcos and ISP Associations
  - The consumer protection associations formal support
- Once the agreement was signed, NIC.br started a national awareness campaign about
  - the importance of these measures and the impact on the consumers
Results: Reduction of Spam Complaints sent to CERT.br
Result: From CBL 1st in 2009 to 25th in 2013

The deadline for the implementation was March 2013

Source of data: Spamhaus CBL (Composite Blocking List) Statistics
http://cbl.abuseat.org/statistics.html
We all need to work on the end user protection

Systems should be less complex – and this requires a technology made for users not geeks...

ISPs and network admins in general need to be more proactive to fight malware and botnets

- RFC 6561: Recommendations for the Remediation of Bots in ISP Networks – examples:
  - iCODE – Australia
  - Botfrei.de – Germany
  - Irish Anti-Botnet Initiative (Botfree.ie) – Ireland
  - Cyber Clean Center (CCC) – Japan
  - Cyber Curing System / e-Call Center 118 – Korea
  - Anti-Botnet Working Group – Netherlands
  - Abuse Information Exchange – Netherlands
  - Autoreporter – Finland
  - U.S. Anti-Bot Code of Conduct (ABCs) for ISPs – US
  - Malware Free Switzerland – Switzerland
  - Advanced Cyber Defence Centre / Botfree.eu – European Union
We need to try and make security appealing

PT: “Cartilha de Segurança para Internet”
http://cartilha.cert.br/

ES: Translation with support from ISOC:
“Cartilla de Seguridad para Internet”
http://cartilla.cert.br/
BCPs need to be easier and provide examples
Thank you!

Dr. Cristine Hoepers
cristine@cert.br

- CERT.br – Computer Emergency Response Team Brazil
  http://www.cert.br/
- NIC.br – Brazilian Network Information Center
  http://www.nic.br/
- CGI.br – Brazilian Internet Steering Committee
  http://www.cgi.br/