Fighting botnets: the need for global cooperation: *Building on EU good practices*

Botnets are networks of ordinary computers, silently hijacked by criminal organisations. They are the cyber-criminal's weapon of choice for serious attacks threatening Europe's economy and the privacy of its citizens – these include spam e-mails, extortion via denial-of-service, identity theft and exploitation for political motives. The total annual global economic loss from malicious software activities is estimated at over 7 billion Euros[1].

What is being done?

There are several promising European initiatives at a national level, including for example:

- ✓ Bot-Frei: a partnership of German ISP's (led by Eco) and the BSI which detects and notifies infected customers and provides disinfection assistance, including a helpline.
- ✓ The Dutch anti-botnet treaty: a partnership of 14 Dutch ISPs and the Telecom Regulatory Authority (OPTA) covering 98% of the Dutch market.
- ✓ The Danish Botnet MoU - a co-operation framework between ISP's and CERTs.
- ✓ The Swedish study on "*Botnets -Hijacked computers in Sweden*".

At a European level, ENISA recently published the results of a wide consultation with all sectors involved in the fight against botnets[2]. This has been taken forward within the European Public Private Partnership for Resilience (EP3R) which is currently planning a **European initiative to fight botnets** based on national EU initiatives and aiming at enhancing cooperation between European ISPs, national authorities and relevant partners.

On an international level, initiatives to fight botnets have been set-up in Japan, Australia and South Korea. The OECD Working Party on Information Security and Privacy (WPISP) is currently examining the role of ISPs in fighting botnets. In the EU-U.S. Working Group on Cyber-security and Cyber-crime, fighting botnets is one of the EU priorities for collaboration.

What are the options for European governments?

Botnets bear many similarities with health epidemics such as H1N1, which are "border-agnostic". Europe has an opportunity to build on the successful initiatives already operating in individual European countries to:

- ✓ **Stimulate the commitment of key national stakeholders** (ISPs, software producers, security companies, public authorities etc.) to join forces to eradicate botnets, in particular, through the European Public Private Partnership for Resilience (EP3R).
- ✓ **Provide a comprehensive policy framework** including appropriate incentives, supportive legislation and suitable technical means **for ISPs, end-users, researchers and software producers** to be able to implement effective defensive measures.

[1] ITU Study on Financial Aspects of Network Security: Malware and Spam. 2008.

[2] See http://www.enisa.europa.eu/act/res/botnets

Who should take responsibility for fighting botnets?

The short answer is everyone. Botnets are part of a highly profitable criminal business model involving many different “production stages”. This business model is highly agile and highly globalised. Every step in the “production process” must be addressed systematically at all levels: local, national, European and increasingly ***at a global level***:

- ✓ **Victims** (of extortion and fraud) should be supported in resisting attacks both technically and with efficient legal recourse and support in prosecuting criminals.
- ✓ **Anti-bot researchers** should be supported by clear and pragmatic legislation.
- ✓ **ISPs** should be supported in detecting infections and helping users to disinfect their machines.
- ✓ **Software producers** and **web service providers** should be supported in the development and implementation of secure software and web applications: vulnerabilities such as flaws in web applications are a major factor in botnet proliferation. Software producers, and in particular web service providers (e.g. banks, search engines etc.), should also contribute to helping users/clients to disinfect their machines.
- ✓ **End-users** should be supported in keeping their machines clean. The threat of botnets means this is no longer just a personal concern, but a social and civic responsibility.

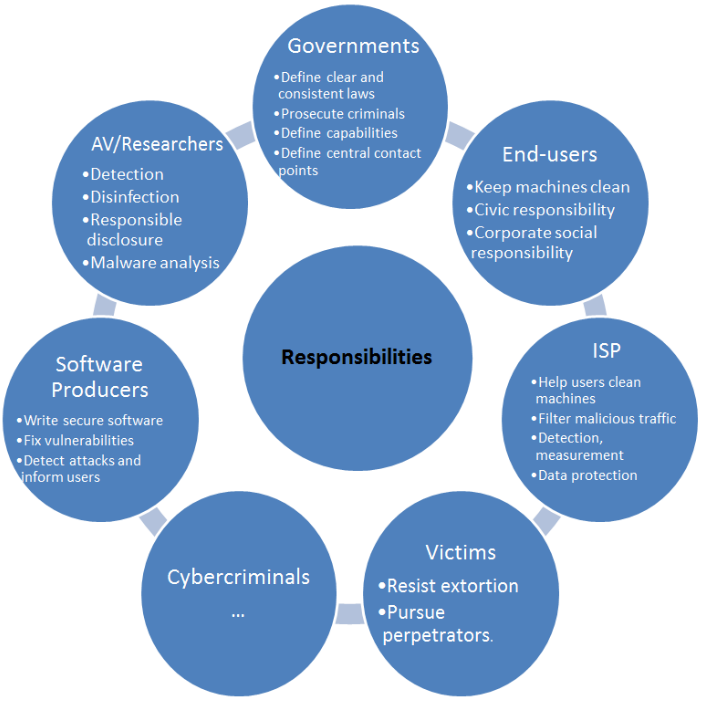
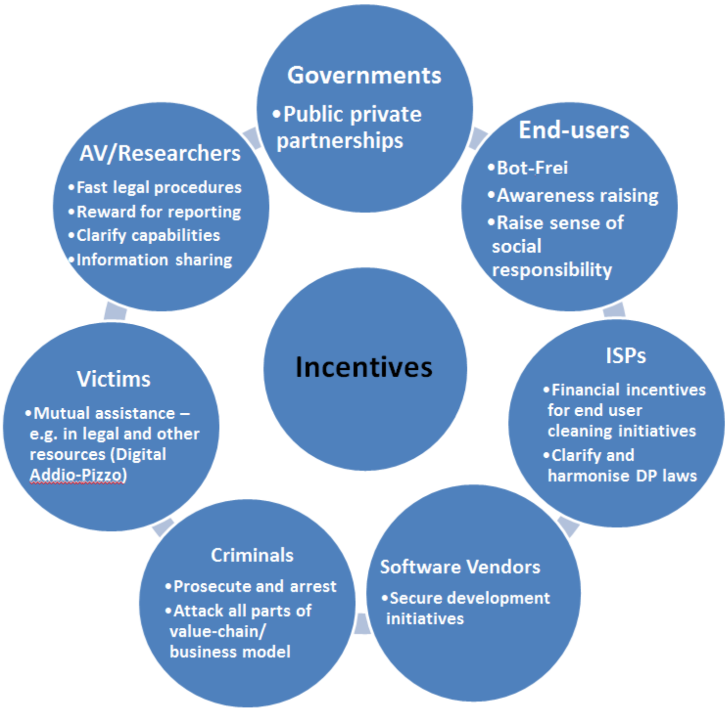


Figure 1: Roles and responsibilities in the fight against botnets



Governments
•Public private partnerships
End-users
•Bot-Frei
•Awareness raising
•Raise sense of social responsibility
ISPs
•Financial incentives for end user cleaning initiatives
•Clarify and harmonise DP laws
Software Vendors
•Secure development initiatives
Criminals
•Prosecute and arrest
•Attack all parts of value-chain/ business model
Victims
•Mutual assistance – e.g. in legal and other resources (Digital Addio-Pizzo)
AV/Researchers
•Fast legal procedures
•Reward for reporting
•Clarify capabilities
•Information sharing
Incentives

Figure 2: ENISA summary of anti-botnet incentives