Press Release

08/03/2011

EPR06/2011

www.enisa.europa.eu

'Facing the cyber-zombies – EU agency gets tough on Botnets

The EU's 'cyber security' Agency, ENISA today published a comprehensive study on the botnet threat (networks of ordinary computers controlled by cybercriminals),and how to address it. The report looks at the reliability of botnet size estimates and makes recommendations for all groups involved in the fight against botnets. Alongside the main report the Agency sets out the top 10 key issues for policymakers in- 'Botnets:10 Tough Questions'

Botnets are networks of computers used without their owner's knowledge for cybercrime such as spamming and the automated theft of valuable data such as credit card information and even politically motivated cyberattacks. "Botnets: 10 Tough Questions" is a policy-level distillation of ENISA's consultation with top experts from all sides of the fight against botnets, including Internet Service Providers (ISPs), security researchers, law enforcement, Computer Emergency Response Teams (CERTs) and anti-virus vendors. It discusses questions such as:

- How much can we trust published figures about botnets?
- What is the role of governments in the fight against botnets?
- What is needed from legislation?
- Where should we invest money most efficiently?

"*The botnet numbers define the political agenda and they determine 100's of millions of Euros of security investments – we* should *understand what is behind them*." says Dr. Giles Hogben, the report Editor. Yet, the report concludes that many botnet figures are likely to be inaccurate and even small numbers of bots can cause severe damage. "*Size is not everything – the number of infected machines alone is an inappropriate measure of the threat*" says Dr. Hogben.

"Botnets: Measurement, Detection, Disinfection and Defence" is a comprehensive report on how to assess botnet threats and how to neutralise them. It includes:

- A survey and analysis of methods for measuring botnet size and how best to assess the threat posed by botnets to different stakeholders.
- A survey and analysis of botnet countermeasures.
- A comprehensive set of 25 different types of best-practices to attack botnets from all angles: neutralising existing botnets, preventing new infections and minimising the profitability of cybercrime using botnets.

The recommendations cover legal, policy and technical aspects of the fight against botnets and give targeted recommendations for different groups involved including:

- The clarification of defensive measures permitted in each member state
- Measures for encouraging users to keep their computers free of botnets.
- Supporting schemes for notification to infected customers by ISP's

The report also emphasises the need for a close international cooperation between governments, technically-oriented, and legislative institutions. "*Global cooperation is indispensable for successful defence against botnets*" says Prof. Udo Helmbrecht, the Executive Director of ENISA.

Both reports will be launched at a conference in Cologne on Wednesday 9th March. A third report focusing on legal issues in the fight against botnets will follow in Q2.

For full papers; Botnets
10 Tough Questions

For interviews, or further details: Ulf Bergstrom, Spokesman, ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143; or Dr. Giles Hogben, Expert, ENISA, giles.hogben Q enisa.europa.eu.