Towards Automated Detection of Peer-to-Peer Botnets: On the Limits of Local Approaches

M. Jelasity and V. Bilicky in 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 09), 2009

August 17, 2009

Summary

The Article provides an analysis of the automated local detection of structured peer-to-peer systems, which implement some techniques to hide their traffic, based on network simulations.

Appreciation

- Good to turn away from finding methods to detect currently used peer-to-peer systems.
  - The development in the area of peer-to-peer systems is very fast.
  - Methods might not work for future versions.

Appreciation

- Critical view on state of the art methods to detect peer-to-peer Botnets.
  - They present simple techniques peer-to-peer systems can implement to avoid detection.
  - Verification for their critical view on these methods.

Criticism

- Claiming without a proof or substantiation very disputable statements about the routing complexity of a P2P system which is using a technique to avoid detection.
- The routing complexity is a very important property of P2P systems.
- When creating a new P2P system this has to be figured out.

Criticism

- Simulation environments are very specific.
  - One fixed peer-to-peer system
  - One fixed network environment
- Based only on this simulations the following is stated as a fact:
  - Automated detection of peer-to-peer botnets "‘cannot be achieved by a local approach"’.

Question

- What do you think? Is it more important to study current peer to peer systems or to look at systems that maybe come up in the future?