

Discovery techniques for P2P Botnets

David Dittrich (U of W), Sven Dietrich (Stevens)

STEVENS
Institute of Technology

Research & Entrepreneurship Day
2009

Introduction

- P2P botnets have become more prevalent
- Discovery is hard due to structure and crypto
- Examples: Storm, Waledac, Conficker, Nugache

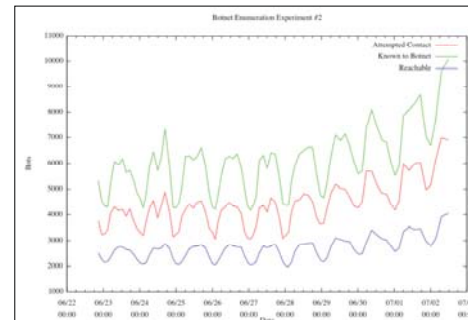
P2P botnet enumeration

- Experiment 1
- Initial enumeration June 2007
- Main purpose: reconnaissance and fixed peer list determination
- Experiments 2 & 3
- Prioritized queue approach
- Emulate the Command and Control protocol (Sybil attack)
- Using 160 peers as starting points, walk the entire network
- Exploit the properties of the botnet to not taint results
- Timings and overlaps
- June 2007 - May 2009

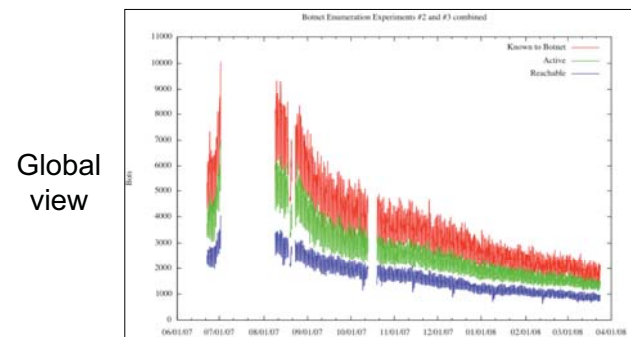
All experiments on live botnet

Results

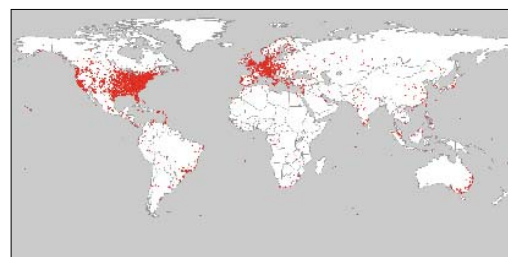
Botnet populations: Experiments 2 & 3



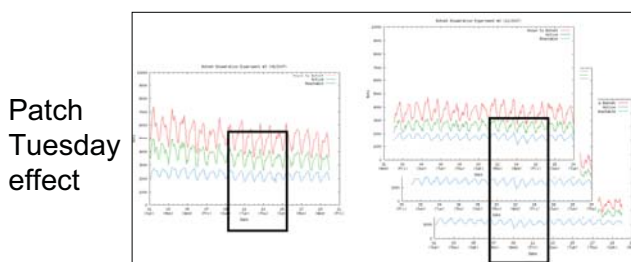
Diurnal effects



Global view



GeoIP view



Patch Tuesday effect

Conclusion

- Size determination is not easy, but relatively accurate, confirmed by third party
- Global effects are observable on botnet
- David Dittrich, Sven Dietrich. Discovery techniques for P2P botnets, Stevens CS Technical Report 2008-4, September 2008. Revised April 2009.