Understanding Large-Scale Spamming Botnets From Internet Edge Sites
Tatsuya Mori, Holly Lovely, Aditya Akella, Akihiro Shimoda, Shigeki Goto
NTT, University of Wisconsin-Madison, Waseda University

Goal
Better understanding of the large-scale spamming botnets from both global and local viewpoints

Lessons learned
• Temporal but significant effectiveness of C&C attack at Internet edge sites.
• Rapid response (version transition) of spamming botnet operation
• Differences of spam contribution from botnet among receiver domains
  → need for global correlation / localization

Approach
• Leverage TCP fingerprint technique
• Correlate SMTP logs and tcpdump traces collected at multiple vantage points

Contributions
1. We extract new variants of TCP fingerprint of the Srizbi bot
2. We evaluate the effectiveness of the C&C (McColo) shut down from Internet edge-sites
3. We reveal the long-term growth and transition of the botnet

Data sets
SMTP logs collected at 3 vantage points
tcpdump traces collected at 4 vantage points

The known and newly extracted TCP fingerprints for Srizbi botnet

Size estimation of botnets with “mark and recapture” method

Effectiveness of C&C Shutdown (2008/11)

Long-term trends

Graphs and tables illustrating the data and findings from the research.