# Of Bees and Botnets

Vijay Sarvepalli(✉)

Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA
vssarvepalli@sei.cmu.edu

Botnets' ability to grow to large sizes, combined with our inability to exhaustively incapacitate them, has forced us to look for more effective methods to model their growth and seek ways to curtail it. Swarm behavior is a stochastic modeling technique based on the collective behavior of swarms. Botnets are like swarms of bees in several ways. For both, a successful hive grows while withstanding losses. In addition, a swarm of honeybees uses distributed decision making [2] similar to a botnet.

The Mirai botnet has been responsible for recent large-scale attacks with its elusive backend of unmanaged Internet of Things and its decentralized self-propagation of infection. This paper explores the swarming behavior of bee colonies as a model for botnets' growth. While there are several differences between this ecological behavior and botnets, the collective behavior of loosely coupled individuals exhibits some commonality that is explored here using a simplified meta-huersitic model. This model can be extended with swarm optimization techniques that can help us prepare to address the more complex botnets of the future.

My modeling uses a beehive with the broad roles of scout bees (infected bot scanners), active foragers (infected bots), and inactive bees (inactive/unreachable bots) to understand a botnet such as Mirai. This meta-heuristic uses an approximation of observed ratios of these roles that make a successful beehive [2]. This is implemented to create a Simulated Bee Colony (SBC) using a simple logic and a computer program written in Python. This logic is represented in Eq. 1, which follows the susceptible–infectious–recovered disease spread model [1].

$$\sum(\tau) = N(1 + \frac{Pscout * Psuccess}{n})^{n\tau} - \mu * N \tag{1}$$

$\sum(\tau)$ is the total size of the botnet at any given time $\tau$, where $N$ is the current size of the botnet, *Psuccess* is the probability of success for infection, *Pscout* is the percentage of devices that are active scanners, $n$ is the number of scan operations per time period $\tau$, and $\mu$ represents the decrease in size of the botnet due to a simulated death or other reduction in hive size. The current model is simple in order to evaluate this meta-heuristic. After validating the stability of the simulation with 10 such simulations, one simulation representing a mid-range of botnet growth was compared to scanning data obtained from a few ISPs. The results show that scanning and growth activity can be reasonably modeled with this logic, excluding factors such as varying loss $\mu$ over time (see Fig. 1). The size of a botnet depends on scanning (exploration) and compromise

M. Dorigo et al. (Eds.): ANTS 2018, LNCS 11172, pp. 436–437, 2018.
https://doi.org/10.1007/978-3-030-00533-7

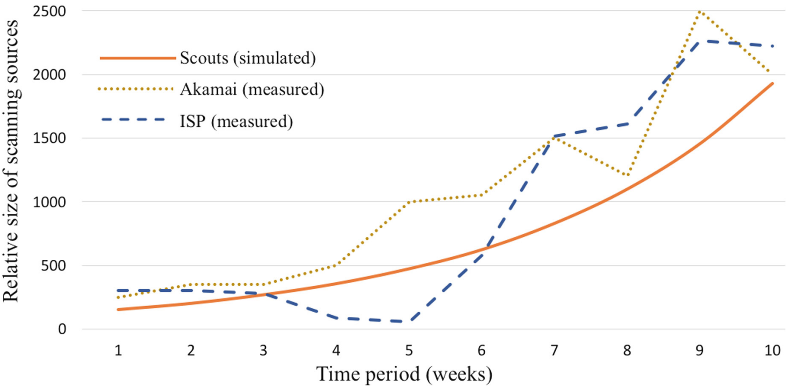

**Fig. 1.** Simulated bee colony vs. measured scanning activities

(exploitation) activities, which are represented by the two probabilities *Pscout* and *Psuccess* in this model.

The following recommendations for the computer security community were developed from these observations:

- ISPs should analyze their dark space for repeated scanners that appear for three or more days and target remediating those identified as "scouts."
- ISPs should monitor outgoing scanning activity and pursue modifying DHCP lease times to reduce sustained scanning activity from these devices.
- Device vendors should identify the types of devices that are becoming effective "scouts" and pursue patching and fixing their vulnerabilities.

Bio-inspired models can be effective ways to analyze and understand botnets' survival techniques that mimic characteristics of a biological system. A stochastic model such as the one proposed illuminates a botnet's strengths and weaknesses. It will allow computer security communities to begin addressing the threat of botnets that perform attacks at large scale.

**Acknowledgments.** I thank Soumya Moitra (Carnegie Melon University), Angelos Stavrou and Constantinos Kolias (George Mason University), and Martin Mckeay (Akamai Technologies) for their input, support, and feedback. This work has been funded by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center DM18-0329.

## References

1. Diekmann, O., Heesterbeek, J.A.P.: Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis and Interpretation, vol. 5. John Wiley & Sons, New York (2000)
2. Janson, S., Middendorf, M., Beekman, M.: Searching for a new home–scouting behavior of honeybee swarms. Behav. Ecol. **18**(2), 384–392 (2006)