Toward Worm Detection in Online Social Networks
Weihua Xu, Fangfang Zhang and Sencun Zhu

Introduction & Motivation

- Online Social Networking (OSN) Websites
  - Popularity: Facebook (>400M users) MySpace (>70M)
  - Attractive targets for worm

- Characteristics of OSNs
  - Small average shortest path length
  - High clustering
  - Scale-free networks

System Design

- System Overview
  - A honeypot-like surveillance network in OSNs
  - A two-level correlation scheme to minimize detection error

- Configuration Module
  - Select as few as possible normal user accounts to deploy decoy friends
  - Leverage topological properties of OSNs

- Evidence Collecting Module
  - Passively collect worm propagation evidence (E.g., worm messages, worm updates)

- Worm Detection Module
  - Two-level spatial-correlation detection
  - Local correlation
  - Network correlation

Evaluation on Flickr Dataset

- Early Warning Detection

<table>
<thead>
<tr>
<th>Worm</th>
<th>Avg. Infection #</th>
<th>Max Infection #</th>
<th>Min Infection #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Koobface</td>
<td>700</td>
<td>1851</td>
<td>2.75</td>
</tr>
<tr>
<td>Mikeyy</td>
<td>1023</td>
<td>2420</td>
<td>2.8</td>
</tr>
</tbody>
</table>

- Impact of Selected User Set Size

- Containment Measures

Fig. 1: Koobface Worm Infection Cycle

Fig. 2: Worm Detection System Overview

Fig. 3: An Example of Two Level Correlation

Fig. 4: Worm Infection Number versus Different Starting Users (Koobface worm case)

Fig. 5: Worm Infection Number versus the Size of Selected Users Set

Fig. 6: Worm Infection versus Different Containment Measures


More information is available: http://www.cse.psu.edu/~szhu/