Laundering Email Spam

Laundering email spam through open-proxies or compromised PCs is a widely-used trick to conceal real spam sources and reduce spamming cost in underground email spam industry.

We revealed one salient characteristic of proxy-based spamming activities, namely packet symmetry, by analyzing protocol semantics and timing causality. Based on packet symmetry, we propose a scheme, called DBSpam, to on-line detect and break spam laundering activities.

Monitoring the bi-directional traffic passing through a network gateway, DBSpam utilizes a simple statistical method, Sequential Probability Ratio Test, to detect the occurrence of spam laundering and suppress it in a timely manner.

Approach and Impact

<table>
<thead>
<tr>
<th>New Approach</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• push the defense line towards spam sources</td>
<td>• reduce email spam</td>
</tr>
<tr>
<td>• no need to scan message contents</td>
<td>• trace out spammer</td>
</tr>
<tr>
<td>• fingerprint spam message</td>
<td></td>
</tr>
</tbody>
</table>

DBSpam

- Deployed on the edge gateway
- Two modules
  - Detection Module
    - Phase one: single out the correlated TCP connections when spamming occurs
    - Phase two: lower the false positives
  - Suppression Module
    - Blocking remote IP addresses
    - Throttling the sending rate