Spamming Botnets: Signatures and Characteristics

Yinglian Xie, Fang Yu, Kannan Achan, Rina Panigrahy, Geoff Hulten, Ivan Osipkov

Presented by Hee Dong Jung
Adapted from slides by Hongyu Gao and Yinglian Xie
Motivation

• Botnets have been widely used for sending spam emails at a large scale
• Detection and blacklisting is difficult as:
  – Each bot may send only a few spam emails
  – Attacks are transient in nature
• Little effort devoted to understanding aggregate behaviors of botnets from perspective of large email servers
Methodology

- Use email dataset from a large email service provider (MSN Hotmail)
- Focus on URLs embedded in email content
- Derive signatures for spam based on URLs
- Detect spam using signatures and find out characteristics of botnets
Methodology

• Challenges:
  – Random, legitimate URLs are added
  – URL obfuscation technique (polymorphic URLs, Redirection)

<table>
<thead>
<tr>
<th>Email 1</th>
<th>Email 2</th>
<th>Email 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.w3.org/wai">http://www.w3.org/wai</a></td>
<td><a href="http://www.w3.org/wai">http://www.w3.org/wai</a></td>
<td><a href="http://www.talkway.com">http://www.talkway.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.dvdfever.co.uk/co1118.shtml">http://www.dvdfever.co.uk/co1118.shtml</a></td>
<td><a href="http://www.dvdfever.co.uk/co1118.shtml">http://www.dvdfever.co.uk/co1118.shtml</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>URLs</th>
<th>Source ASes</th>
<th>URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.lympos.com/n/?167&amp;brokenacclaim">http://www.lympos.com/n/?167&amp;brokenacclaim</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.lympos.com/n/?167&amp;acceptoraudience">http://www.lympos.com/n/?167&amp;acceptoraudience</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://shgeep.info/tota/indexx.html?kjjja.cvqxjby,hvx">http://shgeep.info/tota/indexx.html?kjjja.cvqxjby,hvx</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://shgeep.info/tota/indexx.html?ivx_ceh.cvqxjby,hvx">http://shgeep.info/tota/indexx.html?ivx_ceh.cvqxjby,hvx</a></td>
</tr>
</tbody>
</table>
Is there a way to circumvent any of these steps?
Automatic URL Regular Expression Generation

- Signature Tree Construction

\[
\begin{align*}
    u_1 & : \text{http://deaseda.info/ego/zoom.html?QiQRP_xbZf.CVQjY},hVX \\
    u_2 & : \text{http://deaseda.info/ego/zoom.html?giAfs.CVQjY},hVX \\
    u_3 & : \text{http://deaseda.info/ego/zoom.html?RQbWfeVYZWlfsd.cVQjY},hVX \\
    u_4 & : \text{http://deaseda.info/ego/zoom.html?UbSjWcHC.cVQjY},hVX \\
    u_5 & : \text{http://deaseda.info/ego/zoom.html?VP5_eYVNlS.cVQjY},hVX \\
    u_6 & : \text{http://deaseda.info/ego/zoom.html?QNVRCjgVNSbgfSR.XRW/hVX} \\
    u_7 & : \text{http://deaseda.info/ego/zoom.html?afRZXQ.XRW/hVX} \\
    u_8 & : \text{http://deaseda.info/ego/zoom.html?YcGGA.XRW/hVX} \\
    u_9 & : \text{http://deaseda.info/ego/zoom.html?aeSfLWVYgRIBH.XRW/hVX} \\
\end{align*}
\]

- Regular Expression Generation
  - Detailing → Generalization

\[
\begin{align*}
    N_1 & \quad \text{deaseda.info} \\
    N_2 & \quad /\text{ego/zoom.html?} \quad U_2 = \{u_1, u_2, \ldots, u_3\} \\
    N_3 & \quad /\text{ego/zoom.html?} \quad U_3 = \{u_5, u_7, \ldots, u_9\} \\
    N_4 & \quad /\text{cvqjby.hvx} \quad U_4 = \{u_1, u_2, \ldots, u_4\} \\
\end{align*}
\]

\[
\begin{align*}
    /\text{ego/zoom.html?}*\{1,16\}.xrw,hvx \\
    /\text{ego/zoom.html?}*\{5,16\}.cvqjby.hvx \\
\end{align*}
\]
Datasets and Results

- Able to identify spam emails and related botnet hosts (IP addresses / ASes)

<table>
<thead>
<tr>
<th>Month</th>
<th>Nov 2006</th>
<th>June 2007</th>
<th>July 2007</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CU</td>
<td>RE</td>
<td>CU</td>
<td>RE</td>
</tr>
<tr>
<td>Num. of spam campaigns</td>
<td>1,229</td>
<td>519</td>
<td>1835</td>
<td>591</td>
</tr>
<tr>
<td>Num. of ASes</td>
<td>3,176</td>
<td>1,398</td>
<td>4,495</td>
<td>1,906</td>
</tr>
<tr>
<td>Num. of botnet IPs</td>
<td>88,243</td>
<td>23,316</td>
<td>113,794</td>
<td>19,798</td>
</tr>
<tr>
<td>Num. of spam emails</td>
<td>118,613</td>
<td>26,897</td>
<td>208,048</td>
<td>26,637</td>
</tr>
<tr>
<td>Total botnet IPs</td>
<td>100,293</td>
<td>131,234</td>
<td>113,294</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Some statistics pertaining to the botnets identified by AutoRE.
AutoRE Performance

- Low False Positive Rate (between 0.0015 and 0.0020)
- Regular expressions reduce false positive rates by a factor of 10 to 30
- After generalization, AutoRE can detect 9.9 to 20.6% more spam without affecting false positive rates
Spamming Botnet Characteristics

• Botnet IP addresses are spread across a large number of Ases
• 69% of botnet IP addresses are dynamic IPs; more than 80% of campaigns have at least half their hosts in dynamic IP ranges

<table>
<thead>
<tr>
<th>AS description</th>
<th>AS Number</th>
<th>Number of bot IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea Telecom</td>
<td>4766</td>
<td>15757</td>
</tr>
<tr>
<td>Verizon Internet service</td>
<td>19262</td>
<td>11426</td>
</tr>
<tr>
<td>France Telecom</td>
<td>3215</td>
<td>11303</td>
</tr>
<tr>
<td>China 169-backbone</td>
<td>4837</td>
<td>9960</td>
</tr>
<tr>
<td>Chinanet-backbone</td>
<td>4134</td>
<td>8113</td>
</tr>
</tbody>
</table>
Spamming Botnet Characteristics

• Comparison of Different Campaigns
  – It is uncommon for different spam campaigns to overlap

• Correlation with Scanning Traffic
  – Amount of scanning traffic in Aug is higher than in Nov, when botnet IPs were used to send spam
  – Suggests that botnets could have different phases
Discussion and Conclusion

- AutoRE has potential to work in real-time mode
- Leverages bursty and distributed features of botnet attacks for detection

Major Findings
- Botnet hosts are widespread across Internet, with no distinctive sending patterns when viewed individually
- Existence of botnet spam signatures and feasibility of detecting botnet hosts using them
- Botnets are evolving and getting increasingly sophisticated
Discussion Points

• Do you think “Bursty” and “Distributed” properties represent the spam emails?
  – Are there other properties that should be considered?

• When would this URL based approach not work?
Thank you

Questions?
AutoRE

• Framework for automatically generating URL signatures
• Takes set of unlabeled email messages, produces 2 outputs:
  – Set of spam URL signatures
  – Related list of botnet host IP addresses
• Iteratively selects spam URLs based on distributed yet bursty property of botnets-based spam campaigns
• Uses generated spam URL signatures to group emails into spam campaigns
Group Selector (backup)

- Explores the bursty property of botnet email traffic
- Construct $n$ time windows
- $S_i(k)$ is defined as the total number of IP addresses that sent at least one URL in group $i$ in window $k$
- URL groups with sharp spikes are higher ranked
Automatic URL Regular Expression Generation (backup)

• Signature Quality Evaluation
  – Quantitatively measures quality of signature and discards signatures that are too general
  – Metric: entropy reduction
    • Leverages on information theory to quantify probability of a random string matching a signature
    • Given a regular expression $e$, let $B_e(u)$ and $B(u)$ denote expected # bits to encode a random string $u$ with and without signature
    • Entropy reduction $d(e) = B(u) - B_e(u)$ reflects probability of arbitrary string with expected length allowed by $e$ and matching $e$, but not encoded using $e$
Botnet Validation

• Verify if each spam campaign is correctly grouped together by computing similarity of destination Web pages

• Web pages pointed to by each set of polymorphic URLs are similar to each other, while pages from different campaigns are different.
Spamming Botnet Characteristics

• For each campaign, standard deviation (std) of spam email sending time is computed
  – 50% of campaigns have std less than 1.81 hours
  – 90% of campaigns have std less than 24 hours and likely located at different time zones

• For each campaign, host sending patterns are generally well-clustered
  – Number of recipients per email
  – Connection rate

• Botnet hosts do not exhibit distinct sending patterns for them to be identified