SpamPots Project:
Using Honeypots to Measure the Abuse of End-User Machines to Send Spam

Cristine Hoepers
General Manager
cristine@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

CERT.br - Brazilian National CERT

- Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - **Produce best practices' documents**
  - Help raise the security awareness in the country
  - Maintain public statistics about incidents and abuse

http://www.cert.br/mission.html

AusCERT Conference 2007 - Gold Coast, Australia - May 23, 2007
Our Parent Organization:
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has the main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- to recommend standards for technical and operational procedures
- to establish strategic directives related to the use and development of Internet in Brazil
- to promote studies and technical standards for the network and services’ security in the country
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- to collect, organize and disseminate information on Internet services, including indicators and statistics

http://www.cgi.br/internacional/
AusCERT Conference 2007 - Gold Coast, Australia - May 23, 2007
Agenda

• Motivations
• The architecture
• Data gathered
• Future work

Motivations
The Nature of the Problem

• Spam is a source of
  – Malware
  – Phishing
  – Decrease in productivity (people losing e-mails, etc)
  – Increase in infrastructure investment (filters, bandwidth, etc)

• Congress and regulators
  – Are pressed by the general public to “do something about it”
  – Have several questionable law projects to consider
  – Don’t have data that show the real spam scenario

Different Views, Different Data

• What we “hear”
  – Open proxies are not an issue anymore
  – Only botnets are used nowadays to send/relay spam
  – Brazil is a big “source” of spam

• Our data
  – Spam complaints related to open proxy abuse have increased in the past few years
  – Scans for open proxies are always in the top 10 ports in our honeypots’ network statistics
    http://www.honeypots-alliance.org.br/stats/
Still Lots of Questions

- How to convince business people of possible mitigation measures needs/effectiveness?
  - Port 25 management, e-mail reputation, etc
- Who is abusing our infrastructure? And How?
- Do we have national metrics or only international?
- How can we gather data and generate metrics to help the formulation of policies and the understanding of the problem?

Need to better understand the problem and have more data about it

The SpamPots Project
The SpamPots Project

- Supported and sponsored by NIC.br/CGI.br
  - As part of the Anti-spam Commission work
- Deployment of low-interaction honeypots, emulating open proxy/relay services and capturing spam
  - 10 honeypots in 5 different broadband providers
    - 2 Cable and 3 ADSL
    - 1 residential and 1 business connection each
- Measure the abuse of end-user machines to send spam

End Users Abuse Scenario
Details of the Low-Interaction Honeypots

- **OpenBSD as the base Operating System (OS)**
  - good proactive security features
  - pf packet filter: stateful, integrated queueing (ALTQ), port redirect
  - logs in libpcap format: allows passive fingerprinting

- **Honeyd emulating services**
  - Niels Provos' SMTP and HTTP Proxy emulators - with minor modifications
  - SOCKS 4/5 emulator written by ourselves
  - pretends to connect to the final SMTP server destination and starts receiving the emails
  - doesn't deliver the emails

- **Fools the spammers’ confirmation attempts**
Data Gathered

Total Numbers

Period: June 10, 2006 to April 30, 2007
Days: 325

Emails captured: 370.263.413 (≈ 370M)
Recipients: 3.287.153.093 (≈ 3.2G)
Average recipients/email: ≈ 8.9
Unique IPs seen: 160.502 (≈ 160K)
Unique ASNs: 2813
Unique CCs (Country Codes): 157
Spams Captured per Day

<table>
<thead>
<tr>
<th>#</th>
<th>Country Code</th>
<th>E-mails received</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>TW</td>
<td>281,601,310</td>
<td>76.05</td>
</tr>
<tr>
<td>02</td>
<td>CN</td>
<td>58,912,303</td>
<td>15.91</td>
</tr>
<tr>
<td>03</td>
<td>US</td>
<td>14,939,973</td>
<td>4.03</td>
</tr>
<tr>
<td>04</td>
<td>CA</td>
<td>6,677,527</td>
<td>1.80</td>
</tr>
<tr>
<td>05</td>
<td>KR</td>
<td>1,935,648</td>
<td>0.52</td>
</tr>
<tr>
<td>06</td>
<td>JP</td>
<td>1,924,341</td>
<td>0.52</td>
</tr>
<tr>
<td>07</td>
<td>HK</td>
<td>816,072</td>
<td>0.22</td>
</tr>
<tr>
<td>08</td>
<td>DE</td>
<td>776,245</td>
<td>0.21</td>
</tr>
<tr>
<td>09</td>
<td>BR</td>
<td>642,446</td>
<td>0.17</td>
</tr>
<tr>
<td>10</td>
<td>PA</td>
<td>355,622</td>
<td>0.10</td>
</tr>
</tbody>
</table>
CCs that Injected Most Spam (2/2)


Top 10 ASNs (1/2)

<table>
<thead>
<tr>
<th>#</th>
<th>ASN</th>
<th>ASN Name</th>
<th>E-mails</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>9924</td>
<td>TFN-TW Taiwan Fixed Network</td>
<td>118,773,092</td>
<td>32.08</td>
</tr>
<tr>
<td>02</td>
<td>3462</td>
<td>HINET Data Communication</td>
<td>94,072,091</td>
<td>25.41</td>
</tr>
<tr>
<td>03</td>
<td>17623</td>
<td>CNCGROUP-SZ</td>
<td>49,505,890</td>
<td>13.37</td>
</tr>
<tr>
<td>04</td>
<td>4780</td>
<td>SEEDNET Digital United Inc. (TW)</td>
<td>45,194,157</td>
<td>12.21</td>
</tr>
<tr>
<td>05</td>
<td>9919</td>
<td>NCIC-TW</td>
<td>8,337,948</td>
<td>2.25</td>
</tr>
<tr>
<td>06</td>
<td>4837</td>
<td>CHINA169 - CNCGROUP</td>
<td>6,239,492</td>
<td>1.69</td>
</tr>
<tr>
<td>07</td>
<td>7271</td>
<td>Look Communications (CA)</td>
<td>5,599,442</td>
<td>1.51</td>
</tr>
<tr>
<td>08</td>
<td>7482</td>
<td>Asia Pacific On-line Service (TW)</td>
<td>3,636,788</td>
<td>0.98</td>
</tr>
<tr>
<td>09</td>
<td>18182</td>
<td>Sony Network Taiwan</td>
<td>3,562,012</td>
<td>0.96</td>
</tr>
<tr>
<td>10</td>
<td>18429</td>
<td>EXTRALAN-TW</td>
<td>3,308,528</td>
<td>0.89</td>
</tr>
</tbody>
</table>
Top 10 ASNs (2/2)

TCP Ports Abused Over the Period (1/2)
TCP Ports Abused Over the Period (1/2)

Top Source Operating Systems (1/2)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>E-mails</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>235,990,984</td>
<td>63.74</td>
</tr>
<tr>
<td>Unknown</td>
<td>133,276,691</td>
<td>36.00</td>
</tr>
<tr>
<td>Unix</td>
<td>945,642</td>
<td>0.26</td>
</tr>
<tr>
<td>Other</td>
<td>50,096</td>
<td>0.01</td>
</tr>
</tbody>
</table>

http://www.openbsd.org/cgi-bin/man.cgi?query=pf.os
Future Work

• More comprehensive spam analysis
  – Using Data Mining techniques
  – Determine patterns in language, embedded URLs, etc
  – Phishing and other online crime activities

• Recommend best practices to ISPs
  – port 25 management
  – proxy abuse monitoring

• International cooperation
References

– This presentation -- by the end of the month
  http://www.cert.br/docs/presentations/
– CERT.br
  http://www.cert.br/
– NIC.br
  http://www.nic.br/
– CGI.br
  http://www.cgi.br/
– OpenBSD
  http://www.openbsd.org/
– Honeyd
  http://www.honeyd.org/
– Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/