Using Honeypots to Monitor Spam and Attack Trends

Marcelo H. P. C. Chaves
mhp@cert.br

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

*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
- Establishes collaborative relationships with other entities
- Helps new CSIRTs to establish their activities
- Provides training in incident handling
- Provides statistics and best practices’ documents
- Helps raise the security awareness in the country

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

01- Ministry of Science and Technology
02- Ministry of Communications
03- Presidential Cabinet
04- Ministry of Defense
05- Ministry of Development, Industry and Foreign Trade
06- Ministry of Planning, Budget and Management
07- National Telecommunications Agency
08- National Council of Scientific and Technological Development
09- National Forum of Estate Science and Technology Secretaries
10- Internet Expert
11- Internet Service Providers
12- Telecommunication Infrastructure Providers
13- Hardware and Software Industries
14- General Business Sector Users
15- Non-governamental Entity
16- Non-governamental Entity
17- Non-governamental Entity
18- Non-governamental Entity
19- Academia
20- Academia
21- Academia
Our Parent Organization: CGI.br

Among the diverse responsibilities of The Brazilian Internet Steering Committee – CGI.br, the main attributions are:

- to propose policies and procedures related to the regulation of the 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 (IPs) and the registration of domain names using `<.br>`
- to collect, organize and disseminate information on Internet services, including indicators and statistics
Agenda

Timeline

The Distributed Honeypots Project
   Objective
   Architecture
   Key Points, Benefits and Disavantages
   Statistics

The SpamPots Project
   Objectives and Structure
   Architecture
   Statistics
   Next Steps

References
Timeline

- **March/2002**
  - Honeynet.BR project first honeynet deployed

- **June/2002**
  - Joined the Honeynet Research Alliance

- **September/2003**
  - The “Brazilian Honeypots Alliance – Distributed Honeypots Project” was started
Brazilian Honeypots Alliance
Distributed Honeypots Project
Main Objective

Increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 39 partner’s institutions:
  - Academic, government, industry, telecom and military networks
- Widely distributed across the country
- Based on voluntary work
- Honeypots based on OpenBSD and Honeyd
- Maintain public statistics

http://www.honeypots-alliance.org.br/
### 39 Partners of the Brazilian Honeypots Alliance

<table>
<thead>
<tr>
<th>#</th>
<th>City</th>
<th>Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>São José dos Campos</td>
<td>INPE, ITA</td>
</tr>
<tr>
<td>02</td>
<td>Rio de Janeiro</td>
<td>CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ</td>
</tr>
<tr>
<td>03</td>
<td>São Paulo</td>
<td>ANSP, CERT.br, Diveo, Durand, TIVIT, UNESP, UOL, USP</td>
</tr>
<tr>
<td>04</td>
<td>Campinas</td>
<td>CenPRA, ITAL, UNICAMP</td>
</tr>
<tr>
<td>05</td>
<td>São José do Rio Preto</td>
<td>UNESP</td>
</tr>
<tr>
<td>06</td>
<td>Piracicaba</td>
<td>USP</td>
</tr>
<tr>
<td>07</td>
<td>Brasília</td>
<td>Banco do Brasil, Brasil Telecom, Ministério da Justiça, TCU</td>
</tr>
<tr>
<td>08</td>
<td>Natal</td>
<td>UFRN</td>
</tr>
<tr>
<td>09</td>
<td>Petrópolis</td>
<td>LNCC</td>
</tr>
<tr>
<td>10</td>
<td>Porto Alegre</td>
<td>CERT-RS</td>
</tr>
<tr>
<td>11</td>
<td>Ribeirão Preto</td>
<td>USP</td>
</tr>
<tr>
<td>12</td>
<td>São Carlos</td>
<td>USP</td>
</tr>
<tr>
<td>13</td>
<td>Taubaté</td>
<td>UNITAU</td>
</tr>
<tr>
<td>14</td>
<td>Florianópolis</td>
<td>UFSC DAS</td>
</tr>
<tr>
<td>15</td>
<td>Americana</td>
<td>VIVAX</td>
</tr>
<tr>
<td>16</td>
<td>Manaus</td>
<td>VIVAX</td>
</tr>
<tr>
<td>17</td>
<td>Joinville</td>
<td>UDESC</td>
</tr>
<tr>
<td>18</td>
<td>Lins</td>
<td>FPTE</td>
</tr>
<tr>
<td>19</td>
<td>Uberlândia</td>
<td>CTBC Telecom</td>
</tr>
<tr>
<td>20</td>
<td>Santo André</td>
<td>VIVAX</td>
</tr>
<tr>
<td>21</td>
<td>Passo Fundo</td>
<td>UPF</td>
</tr>
<tr>
<td>22</td>
<td>Curitiba</td>
<td>Onda, PoP-PR, PUCPR</td>
</tr>
<tr>
<td>23</td>
<td>Belém</td>
<td>UFPA</td>
</tr>
<tr>
<td>24</td>
<td>São Leopoldo</td>
<td>Unisinos</td>
</tr>
<tr>
<td>25</td>
<td>Belo Horizonte</td>
<td>Diveo</td>
</tr>
</tbody>
</table>
Key Points to Keep and Reach Partners

We are not offering a “black box”

- They have access to their honeypots
- They can extend the honeypot configuration

The honeypot does not capture production data

- Only data directed to the honeypot is collected

They can use their data freely

- For example, as a complement to their IDS infrastructures

We provide specific information to partners

- Daily summaries (sanitized) – each, combined, correlated

Info exchanged with an encrypted mailing list
Benefits and Disavantages

Short Term Benefits
- Few false positives, low cost and low risk
- Networks originating malicious activities notified
- Production of stats and ability to collect malware samples

Long Term Benefits
- Allow members to improve their expertise in several areas: honeypots, firewall, IDS, OS hardening, PGP, etc
- Improve CERT.br’s relationship with the partners

Disavantages
- Harder to maintain than a “plug and play” honeypot
- Honeypots usually don’t catch attacks targeted to production networks
- Information gathered is limited
Public Statistics: Honeypots Flows

August 08, 2007 – http://www.honeypots-alliance.org.br/stats/
Public Statistics: Port summary (coming soon)

- **Hourly**
  
  17: 2007-08-12 18:00 – 2007-08-13 17:59 (GMT)

- **Weekly**
  
  32: 2007-08-06 00:00 – 2007-08-12 23:59 (GMT)

- **Daily**
  
  12: 2007-08-12 00:00 – 2007-08-12 23:59 (GMT)

- **Monthly**
  
  07: 2007-07-01 00:00 – 2007-07-31 23:59 (GMT)
The SpamPots Project
Using Honeypots to Measure the Abuse of End-User Machines to Send Spam
Objectives and Structure

Objectives

• Better understand the abuse of end-user machines to send spam
  – source, different types, language, etc
• Generate metrics to help the formulation of policies

Structure

• Supported by CGI.br/NIC.br Anti-spam Commission
• 10 honeypots in 5 different broadband providers
  – 1 residential an 1 business connection each
  – based on OpenBSD and Honeyd
  – emulate open proxy/relay services and capture spam
  – do not deliver the emails
Architecture

End users broadband computers

Honeypot emulating an Open Proxy

Computer with Open Proxy

Server:
Collects data daily;
Monitors the honeypots resources.

Computer with Open Proxy

Honeypot emulating an Open Proxy

Mail Server 1

Mail Server N

Victim

Victim

Victim

Spammer

## Statistics: The Big Picture

<table>
<thead>
<tr>
<th>period</th>
<th>2006-06-10 to 2007-07-31</th>
</tr>
</thead>
<tbody>
<tr>
<td>days</td>
<td>417</td>
</tr>
<tr>
<td>emails captured</td>
<td>480.120.724</td>
</tr>
<tr>
<td>recipients</td>
<td>4.307.010.941</td>
</tr>
<tr>
<td>avg. recpts/email</td>
<td>≈ 8.97</td>
</tr>
<tr>
<td>avg. emails/day</td>
<td>1.151.368</td>
</tr>
<tr>
<td>unique IPs seen</td>
<td>209.327</td>
</tr>
<tr>
<td>unique ASNs</td>
<td>2.966</td>
</tr>
<tr>
<td>unique CCs</td>
<td>164</td>
</tr>
</tbody>
</table>
Statistics: Spams captured / day

Emails Received [2006-06-10 -- 2007-07-31]
Statistics: Most frequent ASNs

- Top 10 emails/ASN:

<table>
<thead>
<tr>
<th>#</th>
<th>ASN</th>
<th>AS Name</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>9924</td>
<td>TFN-TW Taiwan Fixed Network / TW</td>
<td>33.77</td>
</tr>
<tr>
<td>02</td>
<td>3462</td>
<td>HINET Data Communication / TW</td>
<td>24.35</td>
</tr>
<tr>
<td>03</td>
<td>17623</td>
<td>CNCGROUP-SZ CNCGROUP / CN</td>
<td>12.97</td>
</tr>
<tr>
<td>04</td>
<td>4780</td>
<td>SEEDNET Digital United / TW</td>
<td>10.04</td>
</tr>
<tr>
<td>05</td>
<td>9919</td>
<td>NCIC-TW / TW</td>
<td>1.91</td>
</tr>
<tr>
<td>06</td>
<td>4837</td>
<td>CHINA169-BACKBONE CNCGROUP / CN</td>
<td>1.77</td>
</tr>
<tr>
<td>07</td>
<td>33322</td>
<td>NDCHOST / US</td>
<td>1.73</td>
</tr>
<tr>
<td>08</td>
<td>4134</td>
<td>CHINANET-BACKBONE / CN</td>
<td>1.29</td>
</tr>
<tr>
<td>09</td>
<td>7271</td>
<td>LOOKAS - Look Communications / CA</td>
<td>1.17</td>
</tr>
<tr>
<td>10</td>
<td>18429</td>
<td>EXTRALAN-TW / TW</td>
<td>1.08</td>
</tr>
</tbody>
</table>
Statistics: Most frequent ASNs (2)

Emails Received / ASN [2006-06-10 -- 2007-07-31]

- ASN 9924 (TFN-TW/TW)
- ASN 3462 (HINET/TW)
- ASN 17623 (CNCGROUP/CN)
- ASN 4780 (SEEDNET/TW)
- ASN 9919 (NCIC-TW/TW)
- ASN 4837 (CHINA169-BACKBONE/CN)
- ASN 33322 (NDCHOST/US)

Others

Months (2006 - 2007)
Statistics: Most frequent CCs

- Top 10 emails/CC:

<table>
<thead>
<tr>
<th>#</th>
<th>emails</th>
<th>CC</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>354,042,709</td>
<td>TW</td>
<td>73.74</td>
</tr>
<tr>
<td>02</td>
<td>77,922,019</td>
<td>CN</td>
<td>16.23</td>
</tr>
<tr>
<td>03</td>
<td>26,384,260</td>
<td>US</td>
<td>5.50</td>
</tr>
<tr>
<td>04</td>
<td>6,680,596</td>
<td>CA</td>
<td>1.39</td>
</tr>
<tr>
<td>05</td>
<td>3,712,431</td>
<td>KR</td>
<td>0.77</td>
</tr>
<tr>
<td>06</td>
<td>3,491,197</td>
<td>JP</td>
<td>0.73</td>
</tr>
<tr>
<td>07</td>
<td>3,085,048</td>
<td>HK</td>
<td>0.64</td>
</tr>
<tr>
<td>08</td>
<td>932,330</td>
<td>DE</td>
<td>0.19</td>
</tr>
<tr>
<td>09</td>
<td>771,130</td>
<td>BR</td>
<td>0.16</td>
</tr>
<tr>
<td>10</td>
<td>617,714</td>
<td>UA</td>
<td>0.13</td>
</tr>
</tbody>
</table>
Statistics: Most frequent CCs (2)

Emails Received / Country Code [2006-06-10 -- 2007-07-31]

- TW
- CN
- US
- CA
- Others

Months (2006 - 2007)
Next Steps

- Comprehensive spam analysis
  - using Data Mining techniques
  - determine patterns in language, embedded URLs, etc
  - phishing and other online crime activities

- Propose best practices to ISPs
  - port 25 management
  - proxy abuse monitoring

- International cooperation
References

- Brazilian Internet Steering Committee – CGI.br
  http://www.cgi.br/

- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/

- Brazilian Honeypots Alliance – Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/

- Honeynet.BR
  http://www.honeynet.org.br/

- Previous presentations about the projects
  http://www.cert.br/presentations/

- Several papers presented at other conferences
  http://www.honeynet.org.br/papers/

- SpamPots Project white paper (in Portuguese)
  http://www.cert.br/docs/whitepapers/spampots/