Preventing your Network from Being Abused by Spammers

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
CERT.br Activities

Created in 1997 as the national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil

- Incident Handling
  - Coordination
  - Facilitation
  - Support
  - Statistics

- Training and Awareness
  - Courses
  - Presentations
  - Documents
  - Meetings

- Network Monitoring
  - Distributed Honeypots
  - SpamPots

International Partnerships

fisl10 – 10º Fórum Internacional Software Livre - June 2009, Porto Alegre, RS
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/
CGI.br and NIC.br Structure

GOVERNMENT (Appointed)  I. E.  CIVIL SOCIETY (Elected)
1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – 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-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

Domain Registration
IP Assignment
Studies and Surveys
About ICT use
Internet Engineering
New Projects
W3C Brazilian Office

Executive Branch
Administrative Support
Legal Counsel
Public Relations

Cert.br
Cetic.br
Ceptro.br
Registro.br

Agenda

• The SpamPots Project
  – 1st Phase Review
  – 2nd Phase

• Port 25 Management
  – Current Scenario
  – Impact
  – Benefits
  – Adoption & Challenges

• User awareness initiatives
Understanding and Reducing the Abuse of Brazilian Broadband Networks for sending Spam: SpamPots Project

1st Phase Review
Motivation (1/3)

• Brazil is a big "source" of spam

• Scans for open proxies are always in the top 10 ports in our honeypots' network statistics

  http://www.honeypots-alliance.org.br/stats/

• Spam complaints related to open proxy abuse have increased in the past few years

• Financial fraud is still using spam
Motivation (2/3)

Spams Reported by SpamCop to CERT.br – Most Common Abuse

Months: January 2006 — May 2009

Open Proxy
Direct Delivery
Spamvertised Website

http://www.cert.br/stats/spam/porcentagens/

fisl10 – 10º Fórum Internacional Software Livre - June 2009, Porto Alegre, RS
“The CBL takes its source data from very large spamtraps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc) and dedicated Spam BOTs which have been abused to send spam, worms/viruses that do their own direct mail transmission (…)”

• Brazil is the leading country on number of IPs listed:
  – complete list has 8,949,708 IPs
  – 1,369,938 (15.31%) from Brazil
  – Other countries with more than 5%: IN (10.35%), RU (8.01%), TR (7.79%) and PL (5.61%)

<table>
<thead>
<tr>
<th>Domain</th>
<th>count</th>
<th>% tot</th>
</tr>
</thead>
<tbody>
<tr>
<td>telebahia.net.br</td>
<td>431122</td>
<td>4.82</td>
</tr>
<tr>
<td>telesp.com.br</td>
<td>278250</td>
<td>3.11</td>
</tr>
<tr>
<td>brasiltelecom.net.br</td>
<td>260306</td>
<td>2.91</td>
</tr>
<tr>
<td>telet.com.br</td>
<td>79963</td>
<td>0.89</td>
</tr>
<tr>
<td>netservicos.com.br</td>
<td>74254</td>
<td>0.83</td>
</tr>
<tr>
<td>gvt.net.br</td>
<td>53777</td>
<td>0.60</td>
</tr>
<tr>
<td>ig.com.br</td>
<td>47858</td>
<td>0.53</td>
</tr>
<tr>
<td>timbrasil.com.br</td>
<td>36499</td>
<td>0.41</td>
</tr>
<tr>
<td>ctbctelecom.net.br</td>
<td>26684</td>
<td>0.30</td>
</tr>
<tr>
<td>embratel.net.br</td>
<td>19150</td>
<td>0.21</td>
</tr>
<tr>
<td>canbrasnet.com.br</td>
<td>18683</td>
<td>0.21</td>
</tr>
<tr>
<td>ig.com</td>
<td>9442</td>
<td>0.11</td>
</tr>
</tbody>
</table>

Data extracted on 2009/06/19 -- http://cbl.abuseat.org/
The SpamPots Project

• Main Goals
  – Have metrics about the abuse of our networks
    • Basically measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
  – Help develop the spam characterization research
  – Measure the abuse of end-user machines to send spam

• Structure of the 1st phase
  – Deployment of 10 low-interaction honeypots, emulating open proxy/relay services and capturing spam
    • 5 broadband providers
    • 1 home and 1 business connection each
Location of the Sensors in the 1st Phase

End users broadband computers

Honeypot emulating an Open Proxy

Computer with Open Proxy

Server:
Collects data daily;
Monitors the honeypots resources.

Mail Server 1

Mail Server N

Victim

Victim

Victim

spammer
Total Data Collected in 466 Days of Operation

<table>
<thead>
<tr>
<th>Data collected by 10 sensors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mails captured (injected):</td>
<td>524,585,779</td>
</tr>
<tr>
<td>Potencial recipients</td>
<td>4,805,521,964</td>
</tr>
<tr>
<td>Average recipients/e-mail</td>
<td>≈ 9.1</td>
</tr>
<tr>
<td>Average captured e-mails/day</td>
<td>≈ 1.2 Million</td>
</tr>
<tr>
<td>Unique IPs that injected spam</td>
<td>216,888</td>
</tr>
<tr>
<td>Unique Autonomous Systems (AS)</td>
<td>3,006</td>
</tr>
<tr>
<td>Unique Country Codes (CCs)</td>
<td>165</td>
</tr>
</tbody>
</table>
# Distribution by Country Code

<table>
<thead>
<tr>
<th>#</th>
<th>CC</th>
<th>E-mails</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>TW</td>
<td>385,189,756</td>
<td>73.43</td>
</tr>
<tr>
<td>02</td>
<td>CN</td>
<td>82,884,642</td>
<td>15.80</td>
</tr>
<tr>
<td>03</td>
<td>US</td>
<td>29,764,293</td>
<td>5.67</td>
</tr>
<tr>
<td>04</td>
<td>CA</td>
<td>6,684,667</td>
<td>1.27</td>
</tr>
<tr>
<td>05</td>
<td>JP</td>
<td>5,381,192</td>
<td>1.03</td>
</tr>
<tr>
<td>06</td>
<td>HK</td>
<td>4,383,999</td>
<td>0.84</td>
</tr>
<tr>
<td>07</td>
<td>KR</td>
<td>4,093,365</td>
<td>0.78</td>
</tr>
<tr>
<td>08</td>
<td>UA</td>
<td>1,806,210</td>
<td>0.34</td>
</tr>
<tr>
<td>09</td>
<td>DE</td>
<td>934,417</td>
<td>0.18</td>
</tr>
<tr>
<td>10</td>
<td>BR</td>
<td>863,657</td>
<td>0.16</td>
</tr>
</tbody>
</table>

Subtotal: 99.50

---

---

fisl10 – 10º Fórum Internacional Software Livre - June 2009, Porto Alegre, RS
## Distribution by Autonomous System

<table>
<thead>
<tr>
<th>#</th>
<th>AS</th>
<th>CC</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>TFN-TW</td>
<td>TW</td>
<td>32.60</td>
</tr>
<tr>
<td>02</td>
<td>HINET</td>
<td>TW</td>
<td>25.04</td>
</tr>
<tr>
<td>03</td>
<td>CNCGROUP</td>
<td>CN</td>
<td>12.43</td>
</tr>
<tr>
<td>04</td>
<td>SEEDNET</td>
<td>TW</td>
<td>10.38</td>
</tr>
<tr>
<td>05</td>
<td>NCIC-TW</td>
<td>TW</td>
<td>1.75</td>
</tr>
<tr>
<td>06</td>
<td>CHINA169</td>
<td>CN</td>
<td>1.72</td>
</tr>
<tr>
<td>07</td>
<td>NDCHOST</td>
<td>US</td>
<td>1.59</td>
</tr>
<tr>
<td>08</td>
<td>CHINANET</td>
<td>CN</td>
<td>1.39</td>
</tr>
<tr>
<td>09</td>
<td>EXTRALAN</td>
<td>TW</td>
<td>1.29</td>
</tr>
<tr>
<td>10</td>
<td>LOOKAS</td>
<td>CA</td>
<td>1.07</td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td></td>
<td><strong>89.26</strong></td>
</tr>
</tbody>
</table>

### Percentage of Emails Received – Over the Period

![Graph showing email distribution over time](image)

---

fisl10 – 10º Fórum Internacional Software Livre - June 2009, Porto Alegre, RS
<table>
<thead>
<tr>
<th>#</th>
<th>TCP Port</th>
<th>Protocol</th>
<th>Usual Service</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>1080</td>
<td>SOCKS</td>
<td>socks</td>
<td>37.31</td>
</tr>
<tr>
<td>02</td>
<td>8080</td>
<td>HTTP</td>
<td>alternate http</td>
<td>34.79</td>
</tr>
<tr>
<td>03</td>
<td>80</td>
<td>HTTP</td>
<td>http</td>
<td>10.92</td>
</tr>
<tr>
<td>04</td>
<td>3128</td>
<td>HTTP</td>
<td>Squid</td>
<td>6.17</td>
</tr>
<tr>
<td>05</td>
<td>8000</td>
<td>HTTP</td>
<td>alternate http</td>
<td>2.76</td>
</tr>
<tr>
<td>06</td>
<td>6588</td>
<td>HTTP</td>
<td>AnalogX</td>
<td>2.29</td>
</tr>
<tr>
<td>07</td>
<td>25</td>
<td>SMTP</td>
<td>smtp</td>
<td>1.46</td>
</tr>
<tr>
<td>08</td>
<td>4480</td>
<td>HTTP</td>
<td>Proxy+</td>
<td>1.38</td>
</tr>
<tr>
<td>09</td>
<td>3127</td>
<td>SOCKS</td>
<td>MyDoom Backdoor</td>
<td>1.00</td>
</tr>
<tr>
<td>10</td>
<td>3382</td>
<td>HTTP</td>
<td>Sobig.f Backdoor</td>
<td>0.96</td>
</tr>
<tr>
<td>11</td>
<td>81</td>
<td>HTTP</td>
<td>alternate http</td>
<td>0.96</td>
</tr>
</tbody>
</table>
Requests to the HTTP and SOCKS Modules

Number of requests received by the modules, divided according to outbound requested connection type:

<table>
<thead>
<tr>
<th>Type</th>
<th>Requests</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect to 25/TCP</td>
<td>89,496,969</td>
<td>97.62</td>
</tr>
<tr>
<td>connect to others</td>
<td>106,615</td>
<td>0.12</td>
</tr>
<tr>
<td>get</td>
<td>225,802</td>
<td>0.25</td>
</tr>
<tr>
<td>errors</td>
<td>1,847,869</td>
<td>2.01</td>
</tr>
<tr>
<td>total</td>
<td>91,677,255</td>
<td>100.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Requests</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect to 25/TCP</td>
<td>46,776,884</td>
<td>87.31</td>
</tr>
<tr>
<td>connect to others</td>
<td>1,055,081</td>
<td>1.97</td>
</tr>
<tr>
<td>get</td>
<td>225,802</td>
<td>0.25</td>
</tr>
<tr>
<td>errors</td>
<td>5,741,908</td>
<td>10.72</td>
</tr>
<tr>
<td>total</td>
<td>53,573,873</td>
<td>100.00</td>
</tr>
</tbody>
</table>
Among the Activities Observed...

• **Main results:**
  – 99.84% of connections originated from abroad
  – Spammers used all the upload bandwidth available
  – More than 90% of spams targeted networks in other countries

• **Among the outgoing activity that was not aimed at port 25/TCP:**
  – attempts to connect to Yahoo! servers using the Yahoo! Messenger Protocol, via the abuse of SOCKS proxies
Current Anti-spam Activities
Data Mining: Characterization of Spam Campaigns

- Frequent Pattern Tree showing different spam campaigns
  - node’s color represents a different feature that varied among the messages at that level
  - diameter of the node is proportional to the log of the frequency of the characteristic in the campaign

- Some characteristics taken into account:
  - Common keywords
  - Message layout
  - Language
  - Encoding type
  - Similar URLs
  - Services abused

Work developed by researchers from the Federal University of Minas Gerais (DCC/UFMG)
Collaboration with TW Authorities

- MoU with TW NCC (National Communications Commission), TWCERT/CC and TWIA (Taiwan Internet Association)
  - Send data weekly about spam coming from and returning to Taiwan
  - They are identifying and shutting down spammers operations
  - We are discussing the implementation of a sensor in Taiwan
Collaboration with JP Authorities

• In the past few months the activities seen changed
  – IPs assigned to Philippines are attempting to send spam to mobile phones in Japan

• JPCERT/CC and the Japanese Embassy in Brazil contacted us regarding "spam coming from Brazil"
  – the data being collected at the active sensors is being sent to them so they can pursue their investigations
  – They are sharing a case study on the success of Port 25 Management adoption in Japan, regarding the abuse of Japanese networks for sending spam
Understanding the Abuse of Worldwide Distributed Networks for sending Spam: SpamPots Project

2nd Phase
Deployment of spampots' sensors worldwide

• Global view of the data
• Help other networks to understand and prevent being abused by spammers
• Better understand the abuse of the Internet infrastructure by spammers
• Use the spam collected to improve antispam filters
• Develop better ways to
  – identify phishing and malware
  – identify botnets via the abuse of open proxies and relays
• Provide data to trusted parties
  – help the constituency to identify infected machines
  – identify malware and scams targeting their constituency
We are Looking for Partners Interested in...

- Receiving data
  - spams, URLs, IPs abusing the sensors, etc
- Hosting a sensor
- Helping to improve the technology
  - Analysis, capture, collection, correlation with other data sources, etc
- All partners will have access to all data if they want
- We are currently working with networks in the following countries/economies: AU, UY, PL, TW, HK and JP.
Preventing the Abuse: Port 25 Management
Current Scenario: The Abuse
Port 25 Management

Differentiate client-server email submission from the email transmission among servers

- The adoption of port 25 management need to be articulated among competing sectors
  - Email providers
    - deploy message submission, typically on port 587/TCP (RFC 4409), and deploy SMTP authentication
  - Broadband/dial-up providers (for end users)
    - prevent email direct delivery (filtering outgoing traffic targetting port 25/TCP)
Port 25 Management: Impact
Port 25 Management: Benefits

- Network provider IP blocks excluded from block lists
- Less end user complaints
- Makes the abuse of the Internet infrastructure for malicious activities (fraud, identity theft, etc) harder
- Enhances the ability of tracking abuse cases
- Acts on the submission, before the message gets in the email infrastructure
- Reduces the international bandwidth consumption by spammers
- Reduces operational costs
  - Spam was pointed out as the main responsible for consuming the largest amount of operational resources on “2008 Worldwide Infrastructure Security Report” (http://www.arbornetworks.com/report)
Port 25 Management: Adoption & Challenges

• Adoption
  – Worldwide
    http://www.antispam.br/admin/porta25/adocao/
  – Brazil
    Sercomtel (Londrina/PR)

• CGI.br’s Resolution CGI.br/RES/2009/001/P
  http://www.cgi.br/regulamentacao/resolucao2009-001.htm

• Challenges
  – Increase on the load of provider’s user support
  – Network providers need to differentiate between end user and business connections
  – Exception handling (outdated/legacy software)
Port 25 Management on Antispam.br

Gerência de Porta 25

Esta parte do site Antispam.br apresenta um conjunto de políticas e padrões, comumente chamados de "Gerência de Porta 25", que podem ser utilizados em redes de usuários finais ou de caráter residencial para:

- mitigar o abuso de serviços abertos e máquinas infectadas para o envio de spam;
- aumentar a rastreabilidade de fraudadores e spammers.

Estes padrões, que procuram diferenciar a submissão do transporte de e-mails, já foram avaliados pela comunidade internet, estão em discussão no Brasil desde 2005 e já são utilizados em redes de banda larga de caráter residencial de diversos países.

Nas subseções a seguir serão abordadas recomendações para a implementação da Gerência de Porta 25/TCP, de modo a evitar que as redes possam ser tão facilmente abusadas por spammers.

Como Ocorre o Abuso das Redes – cenário e estatísticas sobre o abuso de redes brasileiras de usuários finais ou de caráter residencial para o envio de spam.

O que é Gerência de Porta 25 – apresentação das recomendações e padrões que fazer parte do processo de gerência de tráfego de saída para a porta 25/TCP.

Benefícios da Adoção – importância da adoção e benefícios para as redes que adotam o padrão.

Quem Adota ou Recomenda esta Prática – lista de redes que adotaram a gerência de porta 25, bem como surveys e recomendações de adoção por diversos países.

Documentos, Palestras, Howtos e RFCs sobre o Assunto
User Awareness
Antispam.br Website - Malicious Code Through E-mail

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que sejam de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor**: Programa que permite a um invasor retomar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

- **Spyware**: Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma disfarçada e sem autorização.

- **Keylogger**: Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.

- **Screenlogger**: Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

- **Cavalo de Tróia**: Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções maliciosas e sem o conhecimento do usuário.
Os tipos de spam incluem:

1. **Fraudes**
   - Normalmente, são ataques complexos que visam roubar dados pessoais e financeiros.
   - Os atacantes utilizam e-mails para tentar enganar os usuários.
   - Exemplo: golpes (scams) e phishing.

2. **Golpes (Scams)**
   - Situações em que o usuário recebe uma mensagem fraudulentamente.
   - Exemplo: golpe de phishing e golpe de crédito.

3. **Prevenção**
   - É fundamental que os usuários estejam cientes de como identificar e prevenir esses ataques.
   - Dicas e orientações são fornecidas no site.

4. **Bases de Dados**
   - Os dados brutos são armazenados em bases de dados e analisados para detectar atividades suspeitas.

5. **Inteligência Artificial**
   - AIA (Inteligência Artificial) é usada para melhorar a detecção de spam.

6. **Análise de Correio**
   - O conteúdo dos e-mails é analisado para detectar atividades suspeitas.

7. **Modelo de Detecção de Fraudes**
   - Uso de modelos estatísticos para identificar comportamentos fraudulentos.

8. **Filtros de Correio**
   - Filtros de correio são utilizados para separar spam dos e-mails legítimos.

Para obter mais informações, é possível acessar o site: [http://www.antispam.br/tipos/spam/](http://www.antispam.br/tipos/spam/)
Cartoons

- 4 videos – ≈ 4 minutes each
  - The Internet
  - The Intruders
  - Spam
  - The Defense
    - Freely available on the Internet
    - In several formats and resolutions

- English version (subtitles) already available: http://www.antispam.br/videos/english/

- English (voice-over and written texts) to be released very soon

- Q-CERT interested in making an Arabic voice-over
Video 1: The Internet
Video 2: The Intruders

Vírus
Worm
Bot
Spyware
OS INVASORES
ScreenLogger & Keylogger
Cavalo de Tróia

VOCÊ GANHOU A VIAGEM DOS SEUS PONTOS!!!
Video 3: Spam
Video 4: The Defense
Stickers with the Characters
• This presentation (next week)  
  http://www.cert.br/docs/presentations/  

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

• Antispam.br  
  http://www.antispam.br/