Fraud and Phishing in Brazil

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

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

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

- Brazilian National CERT, created in 1997
- Focal point for computer security incident handling
- Provide statistics, best practices and training
- Maintained by the Brazilian Internet Steering Committee
  - composed of 21 members, as follows:

<table>
<thead>
<tr>
<th>sector</th>
<th>representatives</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government</td>
<td>Ministries of Science and Technology, Communications, Defense, Industry, etc, and Telcos Regulatory Agency (ANATEL)</td>
<td>9</td>
</tr>
<tr>
<td>Corporate sector</td>
<td>Industry, Telcos, ISPs, users</td>
<td>4</td>
</tr>
<tr>
<td>NGO’s</td>
<td>Non-profit organizations, etc</td>
<td>4</td>
</tr>
<tr>
<td>Sci. and Tech. Community</td>
<td>Academia</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Internet expert</td>
<td>1</td>
</tr>
</tbody>
</table>
Overview

Short Timeline of Online Fraud in Brazil
Timeline of Online Fraud in Brazil
Current Trends

Current Developments
CERT.br Initiatives

Statistics
Top Trojan Hosting Domains
Trojan Notifications
AV Vendors Efficiency

Brazilian Federal Police Operations
2001 – 2006

Further Developments Needed
Short Timeline of Online Fraud in Brazil
Timeline of Online Fraud in Brazil

2001
- initial deployment of keyloggers via e-mail
- brute force attacks on bank sites

2002 – 2003
- increase in phishing and widespread use of compromised DNS servers

2003 – 2004
- increase in sophisticated phishing
  - phony sites very similar to the real ones
  - data sent from phony sites to collector sites that processed the data and sent results to e-mail accounts
Timeline of Online Fraud in Brazil (cont.)

2005

- traditional phishing and compromised DNS servers were rarely seen
- the criminals sent spams using the names of well-known entities or popular sites (government, telecom, airline companies, charity institutions, reality shows, e-commerce, etc), as well as varied themes (elections, terrorist attacks, tsunami, fraud warnings, erotic photos, etc)
- these spams had links to trojan horses hosted at various sites
- the victim rarely associated the spam with a banking fraud
Current Trends
2006
Current Trends

Traditional phishing and compromised DNS servers continue to be rarely seen.

The current scheme is:

- spams using even more varied themes
  - usually, the moment dictates what criminals will use
- the spams have links to trojan horses hosted at various sites, but we are observing a considerable increase in the use of:
  - trojan downloaders that lead to the real trojans
  - file hosting sites that masquerade common binary extensions:
    - http://www.z05.zupload.com/dl.php?id=5314
The victim rarely associates the spam with a banking fraud.

Once installed, the trojan has the ability to:

- monitor the victim’s computer looking for accesses to Brazilian well-known banks
- capture keystrokes and mouse events, as well as screen snapshots
- overlap portions of the victim’s screen, hiding information
- send captured information, such as account numbers and passwords, to collector sites or e-mail accounts
Trojan Worm: a case study

18th of April, 2006: trojan incident reported to CERT.br

- 1st infection vector is unknown
- odd netbios traffic generated by infected machines
- AV signatures: too vague or “no virus found”

20th of April, 2006: specific AV signatures

- Net-Worm.Win32.Banker.a (and others)

Artifact Analysis*

- propagation method: looks for Windows opened shares, tries to copy itself to startup directories
- path is hardcoded: works in Brazilian Windows machines
- trojan capabilities: monitors Web activities, overlaps victim’s screen, captures and sends data via e-mail

* CERT.br would like to thank Visanet CSIRT staff for the analysis
Current Developments
CERT.br Initiatives

Trojan notification and submission system

emails

**trojanfilter**
Extract suspicious URLs from emails

**sm2av**
Select new malware from malware´s list
Send malware copy to each AV vendor that does not detect the malware yet

malware files (confirmed)

**trojancheck**
Fetch and store malware candidate
Using AV, confirm if file is really a malware
Create a list with the confirmed URLs

list entry
IP, date, URL, AV signature

**notify**
Get IP contacts
Create email with the list entry data and a email template
Send notification asking to remove the malware

email with the malware copy

**ISTRonline**
Try to fetch malware in order to check if it is still online
Update stats DB including the new date and status of the malware URL

add new URLs

email with the notification
CERT.br Initiatives (cont.)

Actions:

- notifying sites hosting trojans
- sending undetected trojan samples to 28 AV vendors
  - aim is to increase AV effectiveness
- the documents aimed to home users were revised, focusing on Internet frauds and social engineering

Task force between CERT.br and 9 biggest banks:

- PGP mailing list maintained by CERT.br
- CERT.br facilitates exchange of technical information
- banks coordinate efforts with the proper law enforcement agency for each case
Statistics
Top Trojan Hosting Domains

Number of times a domain was referenced in spams, and was hosting a trojan candidate

- 2005-04-01 – 2006-04-30 → 1063321 e-mails, 1251579 URLs

<table>
<thead>
<tr>
<th>number</th>
<th>domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>235124</td>
<td>America Online *</td>
</tr>
<tr>
<td>94624</td>
<td>GratisWeb **</td>
</tr>
<tr>
<td>24656</td>
<td>webcindario.com</td>
</tr>
<tr>
<td>21420</td>
<td>sapo.pt</td>
</tr>
<tr>
<td>20365</td>
<td>symantek.us</td>
</tr>
<tr>
<td>19655</td>
<td>spectrogariaclips.inf.br</td>
</tr>
<tr>
<td>14097</td>
<td>thefilebucket.com</td>
</tr>
<tr>
<td>12607</td>
<td>aocusa.com</td>
</tr>
<tr>
<td>10789</td>
<td>ripway.com</td>
</tr>
<tr>
<td>9985</td>
<td>terra.com.br</td>
</tr>
</tbody>
</table>

* aol.{co.uk,com.au,com,de,com.br,com.mx,ca}, netscape.com, americaonline.com.{ar,mx,br}

** gratisweb.com, wanadoo.es, telepolis.com
## Trojan Notifications

**Summary: 2005-04-01 – 2006-04-30**

<table>
<thead>
<tr>
<th>counter</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>domains</td>
<td>3807</td>
</tr>
<tr>
<td>contacts</td>
<td>1782</td>
</tr>
<tr>
<td>extensions</td>
<td>45</td>
</tr>
<tr>
<td>filenames</td>
<td>9520</td>
</tr>
<tr>
<td>hosts</td>
<td>6137</td>
</tr>
<tr>
<td>IP addresses</td>
<td>3166</td>
</tr>
<tr>
<td>country codes</td>
<td>68</td>
</tr>
<tr>
<td>e-mails sent</td>
<td>15556</td>
</tr>
<tr>
<td>unique URLs</td>
<td>24005</td>
</tr>
<tr>
<td>AV signatures</td>
<td>1546</td>
</tr>
</tbody>
</table>

Total amount of URLs notified = 32648 (with repetition)
Trojan Notifications (cont.)


<table>
<thead>
<tr>
<th>number</th>
<th>(%)</th>
<th>domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>9667</td>
<td>29.61</td>
<td>America Online*</td>
</tr>
<tr>
<td>6656</td>
<td>20.39</td>
<td>GratisWeb**</td>
</tr>
<tr>
<td>1012</td>
<td>03.10</td>
<td>webcindario.com</td>
</tr>
<tr>
<td>433</td>
<td>01.33</td>
<td>rapidupload.com</td>
</tr>
<tr>
<td>234</td>
<td>00.72</td>
<td>terra.com.br</td>
</tr>
<tr>
<td>200</td>
<td>00.61</td>
<td>uol.com.br</td>
</tr>
<tr>
<td>180</td>
<td>00.55</td>
<td>unlugar.com</td>
</tr>
<tr>
<td>168</td>
<td>00.51</td>
<td>yahoo.com.br</td>
</tr>
<tr>
<td>163</td>
<td>00.50</td>
<td>100free.com</td>
</tr>
<tr>
<td>161</td>
<td>00.49</td>
<td>beian.gov.cn</td>
</tr>
</tbody>
</table>

* aol.{co.uk,com.au,com,de,com.br,com.mx,ca}, netscape.com, americaonline.com.{ar,mx,br}
** gratisweb.com, wanadoo.es, telepolis.com
Trojan Notifications (cont.)

Top 10 extensions

Notifications x Extensions [2005-04-01 -- 2005-12-31]

<table>
<thead>
<tr>
<th>Extension</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>exe</td>
<td>14769</td>
</tr>
<tr>
<td>scr</td>
<td>4016</td>
</tr>
<tr>
<td>zip</td>
<td>419</td>
</tr>
<tr>
<td>jpg</td>
<td>221</td>
</tr>
<tr>
<td>com</td>
<td>30</td>
</tr>
<tr>
<td>rar</td>
<td>30</td>
</tr>
<tr>
<td>gif</td>
<td>21</td>
</tr>
<tr>
<td>js</td>
<td>15</td>
</tr>
<tr>
<td>php</td>
<td>15</td>
</tr>
<tr>
<td>html</td>
<td>14</td>
</tr>
</tbody>
</table>

Other extensions:
- txt, bmp, cmd, png, dll, conf, klg, swf, bat, tmp

Notifications x Extensions [2006-01-01 -- 2006-04-30]

<table>
<thead>
<tr>
<th>Extension</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>exe</td>
<td>7582</td>
</tr>
<tr>
<td>scr</td>
<td>3853</td>
</tr>
<tr>
<td>php</td>
<td>666</td>
</tr>
<tr>
<td>cmd</td>
<td>282</td>
</tr>
<tr>
<td>zip</td>
<td>247</td>
</tr>
<tr>
<td>jpg</td>
<td>136</td>
</tr>
<tr>
<td>com</td>
<td>68</td>
</tr>
<tr>
<td>bmp</td>
<td>51</td>
</tr>
<tr>
<td>rar</td>
<td>27</td>
</tr>
<tr>
<td>klg</td>
<td>18</td>
</tr>
</tbody>
</table>

Other extensions:
- kbc, gif, tar, wmf, txt, avi, bat, klb, db, swf, asp, bin, cab, dll, html, ocx, pit, src
Trojan Notifications (cont.)

Top 10 country codes

Notifications x Country Codes [2005-04-01 -- 2005-12-31]

- US: 11508 (53.69%)
- ES: 3240 (16.52%)
- BR: 2029 (10.35%)
- KR: 344 (1.75%)
- GB: 314 (1.60%)
- DE: 279 (1.42%)
- RU: 245 (1.25%)
- CA: 240 (1.22%)
- IT: 231 (1.18%)
- FR: 187 (0.95%)

Notifications x Country Codes [2006-01-01 -- 2006-04-30]

- US: 5605 (42.98%)
- ES: 3547 (27.20%)
- BR: 947 (7.26%)
- RU: 431 (3.31%)
- CN: 409 (3.14%)
- KR: 390 (2.99%)
- IT: 261 (2.00%)
- PT: 228 (1.75%)
- DE: 207 (1.59%)
- AR: 204 (1.56%)
Trojan Notifications (cont.)

Top 10 Signatures


1. Trojan-Spy.Win32.Banker: 10067
2. Trojan-Spy.Win32.Bancos: 8617
3. Trojan-Downloader:Win32.Banload: 4060
4. Trojan-Downloader:Win32.Delf: 1709
5. Trojan-Downloader:Win32.Dadobra: 1343
8. Trojan-Spy.Win32.Delf: 318
10. Trojan-Downloader:Win32.Delf: 126

Signatures source: Kaspersky Lab
AV Vendors Efficiency


- sent a total of 18665 samples to AV vendors

<table>
<thead>
<tr>
<th>Antivirus Vendor</th>
<th>samples</th>
<th>undetected</th>
<th>detected</th>
<th>detection rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor A</td>
<td>18634</td>
<td>1913</td>
<td>16721</td>
<td>89.73</td>
</tr>
<tr>
<td>Vendor B</td>
<td>5653</td>
<td>1020</td>
<td>4633</td>
<td>81.96</td>
</tr>
<tr>
<td>Vendor D</td>
<td>18519</td>
<td>5475</td>
<td>13044</td>
<td>70.44</td>
</tr>
<tr>
<td>Vendor E</td>
<td>18652</td>
<td>6240</td>
<td>12412</td>
<td>66.55</td>
</tr>
<tr>
<td>Vendor F</td>
<td>18665</td>
<td>6857</td>
<td>11808</td>
<td>63.26</td>
</tr>
<tr>
<td>Vendor G</td>
<td>18348</td>
<td>6750</td>
<td>11598</td>
<td>63.21</td>
</tr>
<tr>
<td>Vendor H</td>
<td>18666</td>
<td>7324</td>
<td>11342</td>
<td>60.76</td>
</tr>
<tr>
<td>Vendor I</td>
<td>7474</td>
<td>3160</td>
<td>4314</td>
<td>57.72</td>
</tr>
<tr>
<td>Vendor K</td>
<td>14603</td>
<td>8873</td>
<td>5730</td>
<td>39.24</td>
</tr>
<tr>
<td>Vendor L</td>
<td>18658</td>
<td>11623</td>
<td>7035</td>
<td>37.71</td>
</tr>
<tr>
<td>Vendor N</td>
<td>18371</td>
<td>12866</td>
<td>5505</td>
<td>29.97</td>
</tr>
<tr>
<td>Vendor O</td>
<td>18606</td>
<td>13084</td>
<td>5522</td>
<td>29.68</td>
</tr>
<tr>
<td>Vendor P</td>
<td>14126</td>
<td>10162</td>
<td>3964</td>
<td>28.06</td>
</tr>
<tr>
<td>Vendor Q</td>
<td>18541</td>
<td>13395</td>
<td>5146</td>
<td>27.75</td>
</tr>
<tr>
<td>Vendor T</td>
<td>18652</td>
<td>14140</td>
<td>4512</td>
<td>24.19</td>
</tr>
<tr>
<td>Vendor Y</td>
<td>18469</td>
<td>16713</td>
<td>1756</td>
<td>9.51</td>
</tr>
<tr>
<td>Vendor Z</td>
<td>15784</td>
<td>14517</td>
<td>1267</td>
<td>8.03</td>
</tr>
</tbody>
</table>
AV Vendors Efficiency (cont.)

Trojan Samples Sent [2005-04-11 -- 2006-04-30]

Vendor A: Black
Vendor H: Green
Vendor K: Red
Vendor N: Blue
Vendor T: Purple
Vendor Y: Orange
Vendor Z: Pink

Weeks (2005 - 2006)
Brazilian Federal Police
Operations to Fight Online Fraud
Federal Police Operations

2001: Operation Cash Net (07/Nov)
- modus operandi:
  - spams poorly written
  - 1st trojan implementations → rudimentary keyloggers
  - brute force attacks when passwords not available
- performed simultaneously in 2 states
- 70 police officers, 17 people arrested
- U$46 million stolen (estimated)

2003: Operation “Cavalo de Tróia I” (05/Nov)
- modus operandi:
  - spams / phony sites / trojans → {key,screen}loggers
  - DNS compromises widely used (“pharming”)
- performed simultaneously in 4 states
- 200 police officers, 30 arrest warrants, 27 people arrested
- U$14 million stolen (estimated)
Federal Police Operations (cont.)

2004: Operation “Cavalo de Tróia II” (20/Oct)

- criminal organization:
  - programmers
    - sophisticated trojans → \{key,screen\}loggers
  - mules
    - locals → drop accounts for small percentages
    - local commerce → payments
  - huge expenses with cars, motorcycles, big parties
  - fraud toolkit (including notebook, programs, howtos)

- performed simultaneously in 4 states
- over 80 police officers, and 90 arrest warrants
- 64 people arrested
- U$110 million stolen (estimated)
Federal Police Operations (cont.)

2005: Operation “Pégasus” (25/Aug)
- even more sophisticated trojans
  - keyloggers + screenloggers + screen overlapping
- performed simultaneously in 8 states
- 400 police officers, 100 arrest warrants, 85 people arrested
- U$33 million stolen (estimated)

2006: Operation Scan (14/Feb)
- performed simultaneously in 7 states
- over 300 police officers
- leader was 19 years old
- 63 people arrested (at least 9 of them minors)
- U$4.7 million stolen (estimated)
Further Developments Needed
Further Developments Needed

AV software need to better detect trojans

- just 1 AV with detection rate of 90%
- 70% of AV’s with detection rates of less than 40%
- most used defense among end users

ISPs need to be more proactive

- check files at upload time and periodically after upload

More efforts to block spam at its source

- working in some technical solutions with telcos and ISPs

Better international cooperation
Related Links

• This presentation can be found at:
  http://www.cert.br/docs/presentations/

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

• Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/