SBSEG 2015

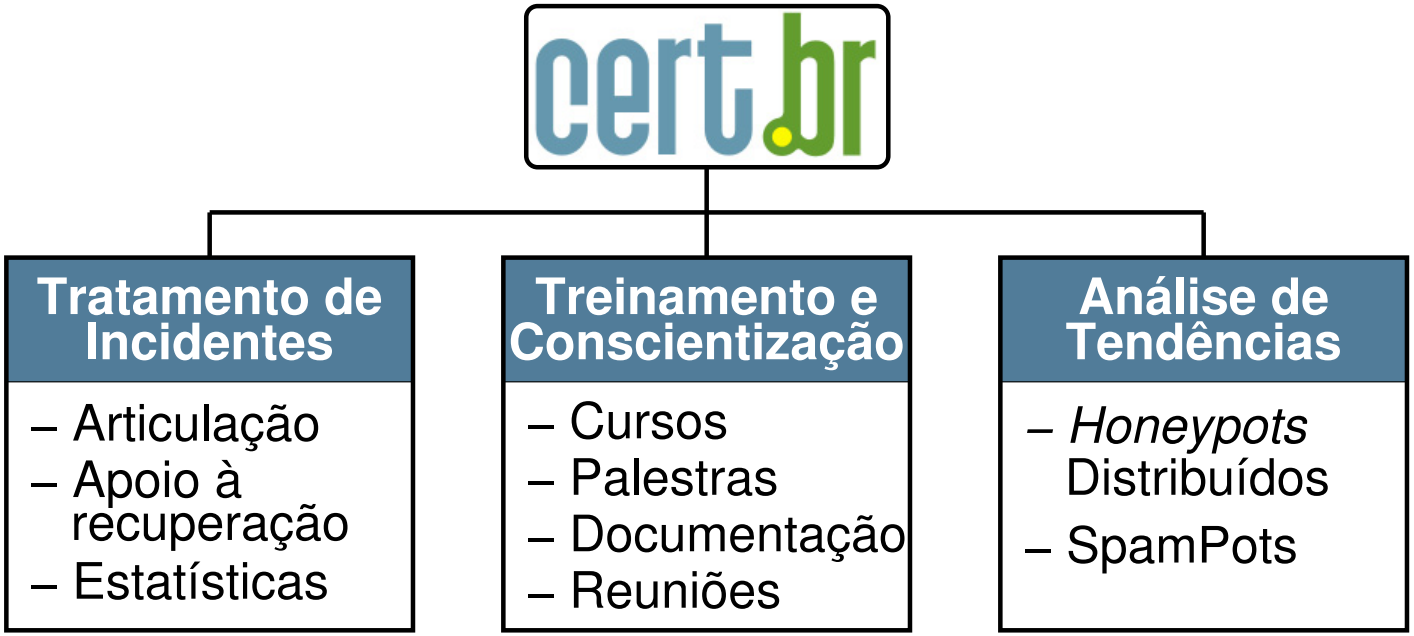
Florianópolis, SC

10 de novembro de 2015

Segurança na Internet: Tendências e Desafios

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

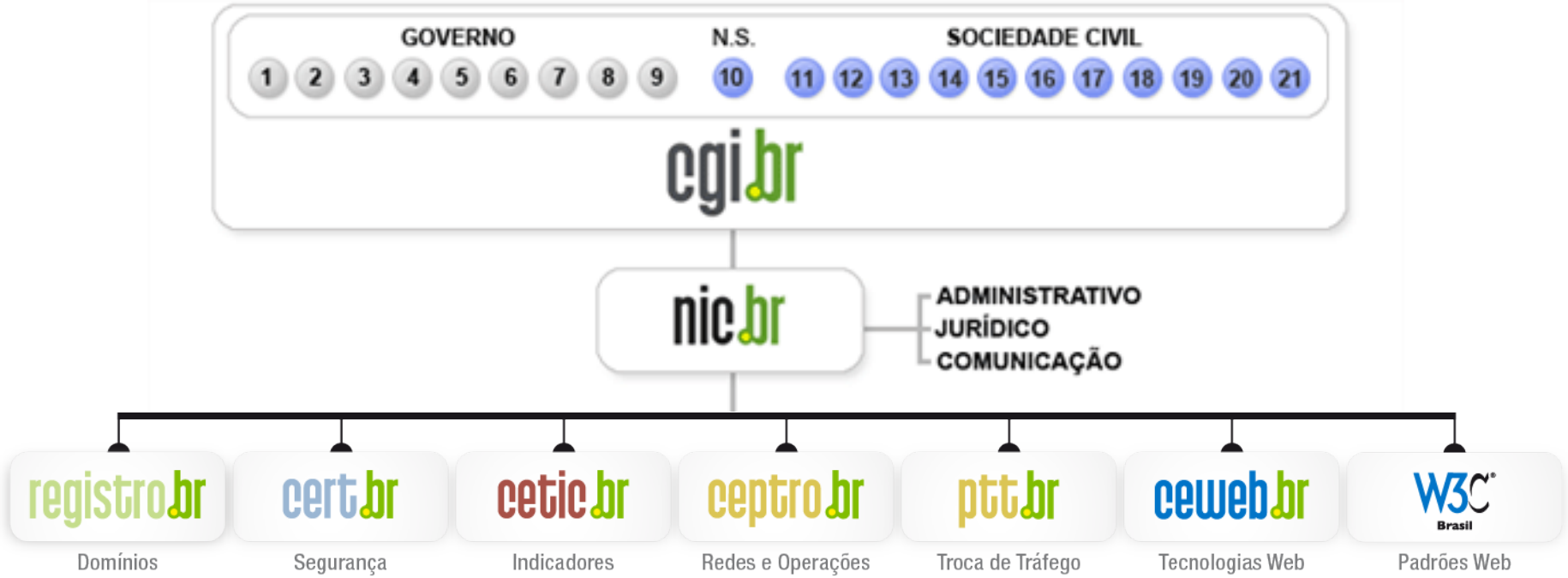
The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre/

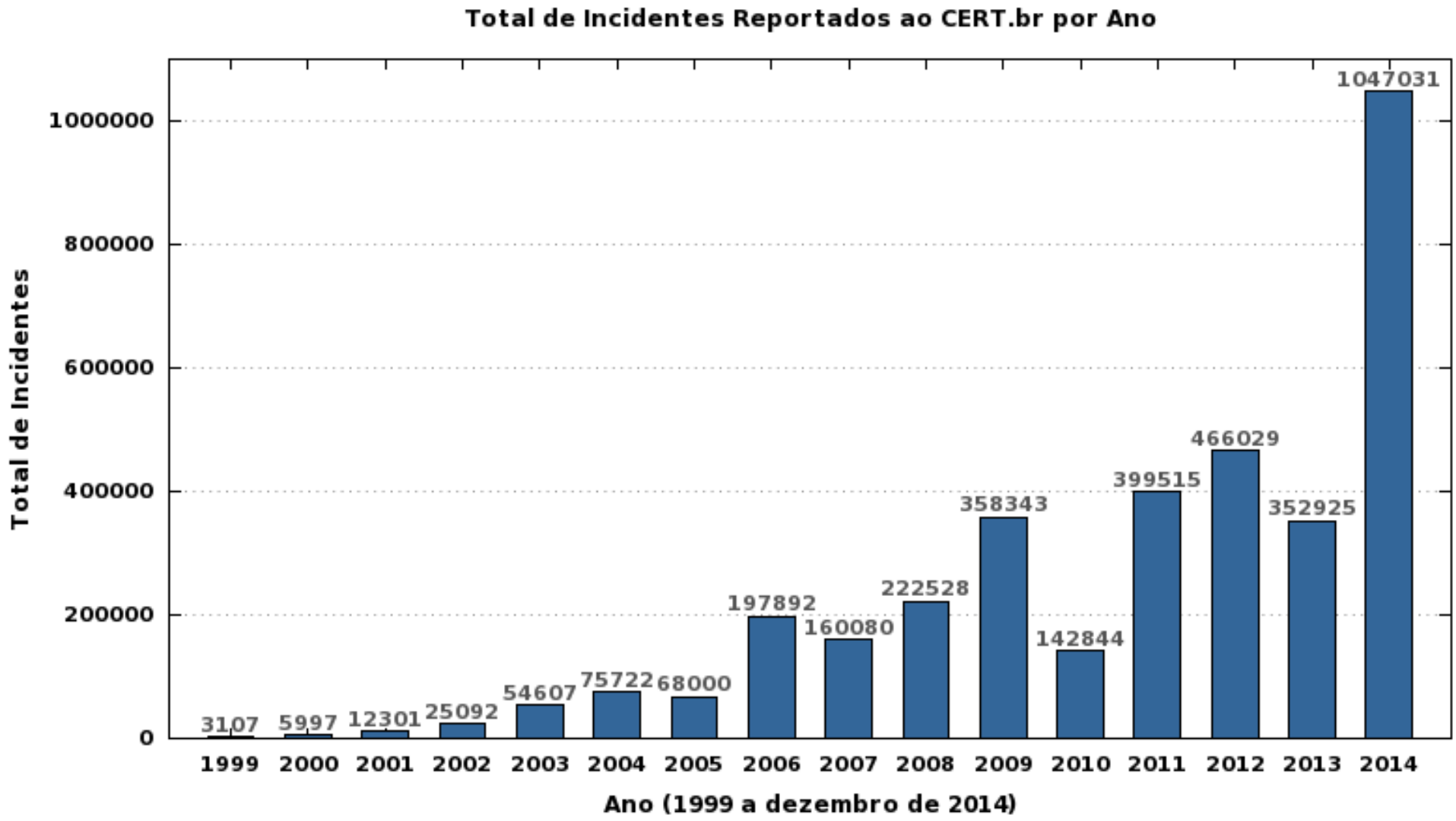
Agenda

- **Cenário e Tendências**
- **Desafios**
  - Como melhorar o cenário
- **Projetos conduzidos pelo CERT.br**
- **Questões éticas**

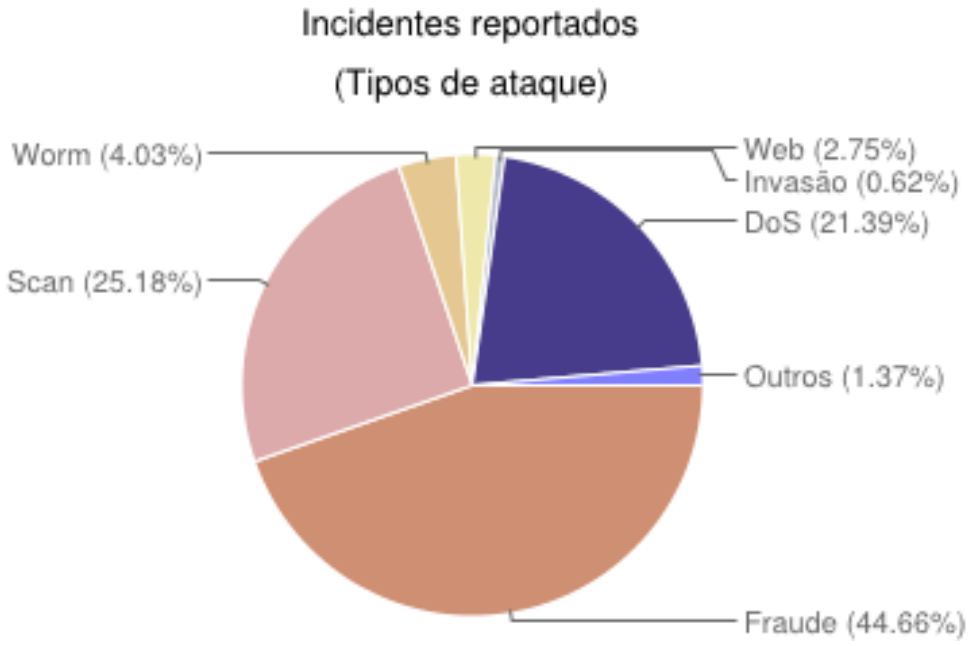
Cenário e Tendências

cert.br nic.br cgi.br

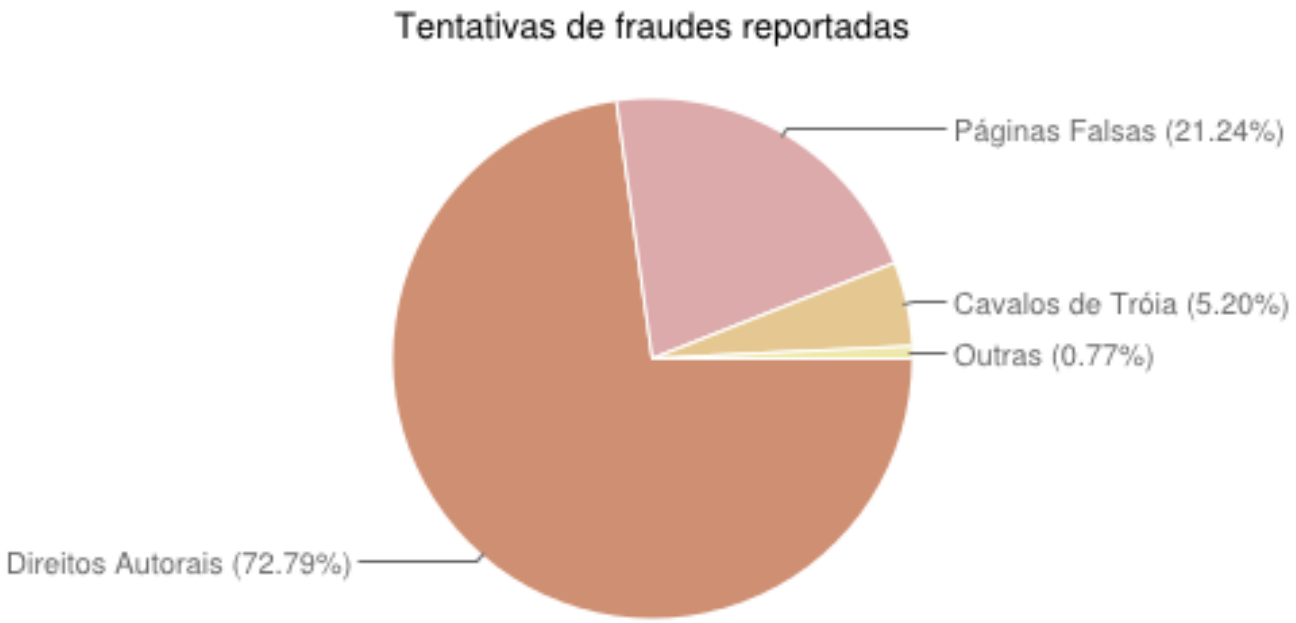
Estatísticas CERT.br



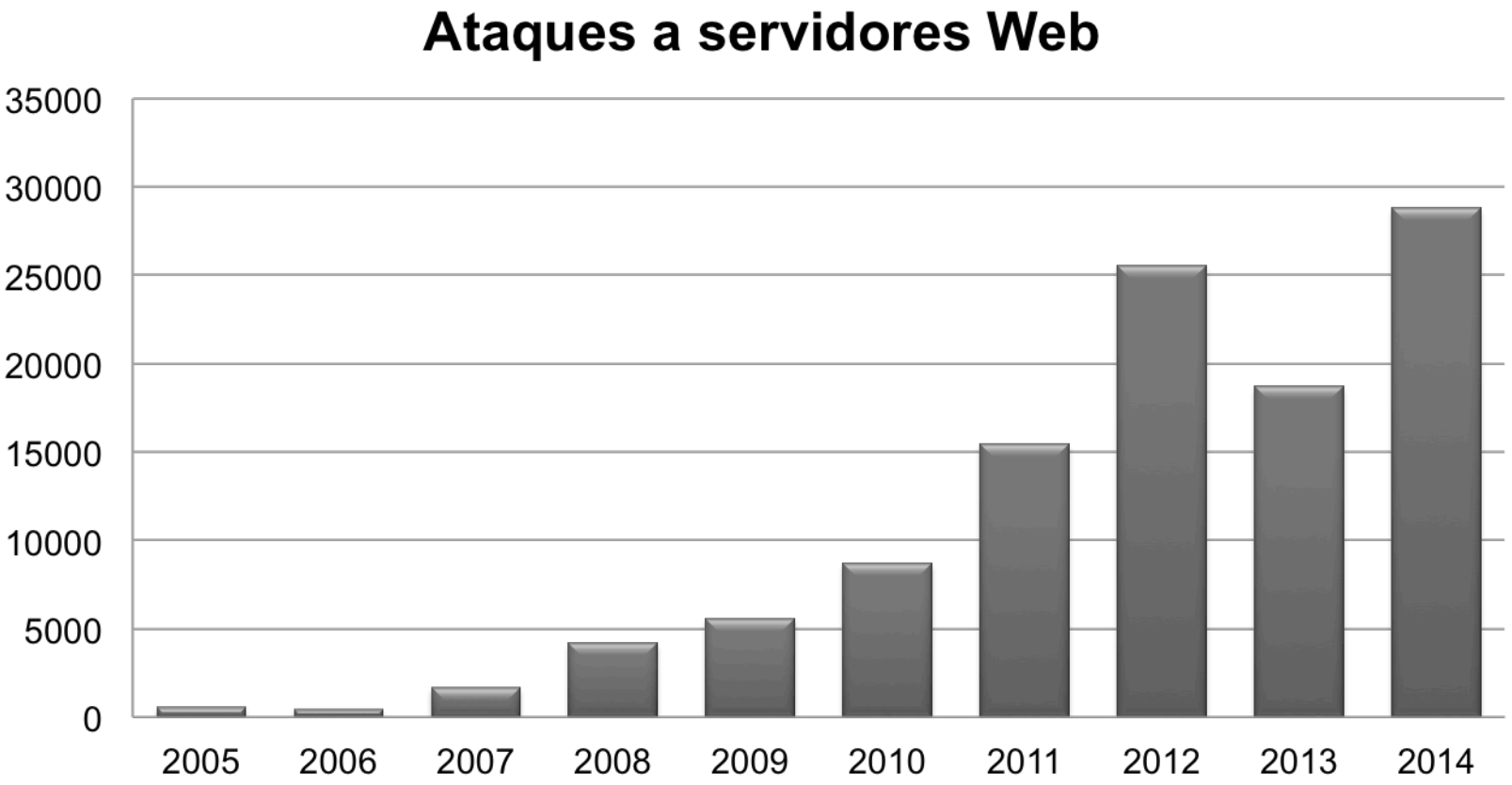
Tipos de ataque – 2014



Tentativas de fraudes reportadas – 2014

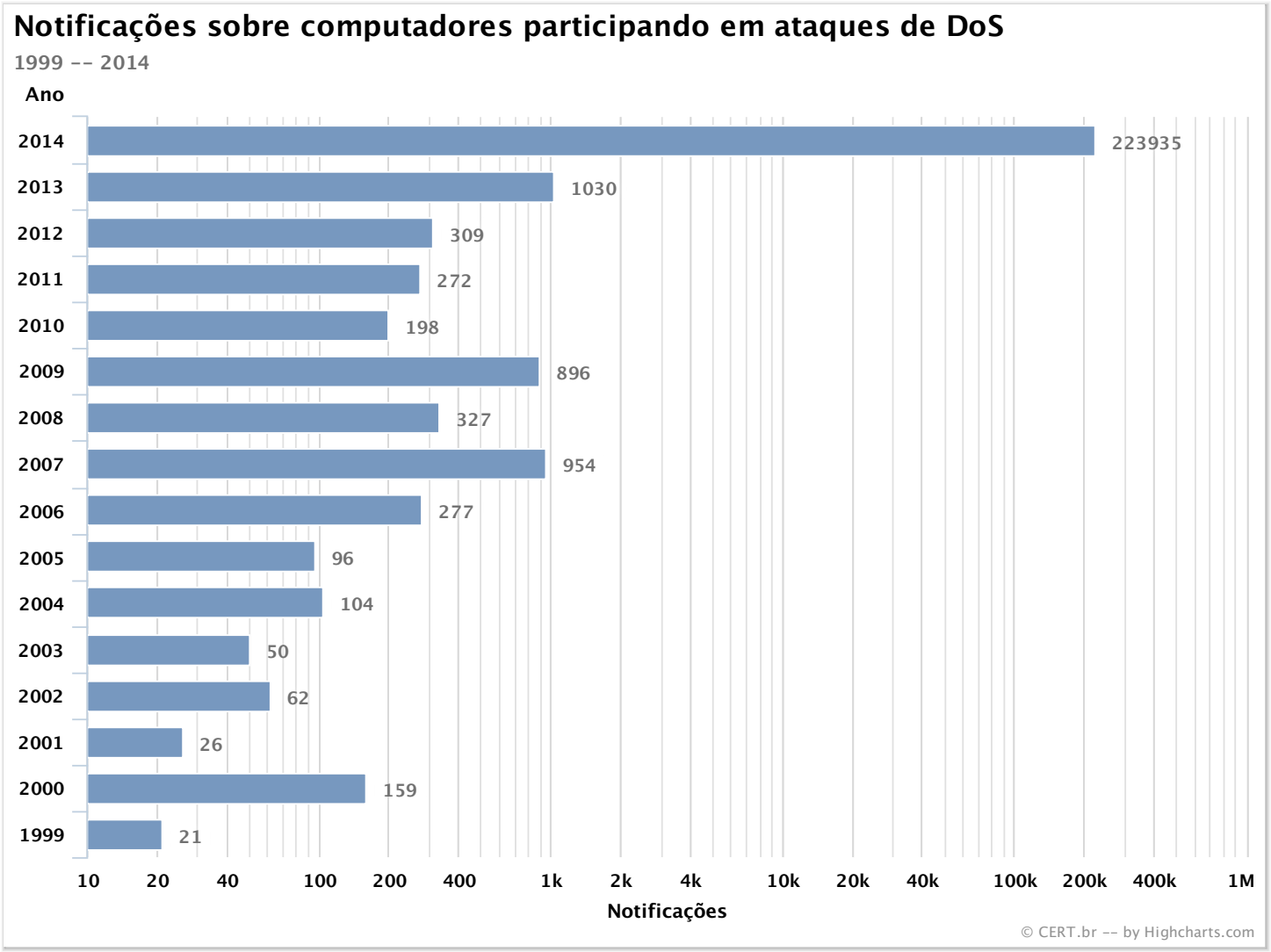


Ataques a servidores Web



Ataques visando o comprometimento de servidores Web ou desfigurações de páginas na Internet
http://www.cert.br/stats/incidentes/

DDoS


Notificações sobre computadores participando em ataques de DoS
1999 -- 2014
Ano
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003
2002
2001
2000
1999
223935
1030
309
272
198
896
327
954
277
96
104
50
62
26
159
21
10
20
40
100
200
400
1k
2k
4k
10k
20k
40k
100k
200k
400k
1M
Notificações
© CERT.br -- by Highcharts.com

DDoS

- **Ataques com amplificação são triviais**
  - serviços UDP permitindo abuso
    - SNMP, SSDP, DNS recursivo aberto
- **Ataques dificilmente são menores que 50Gbps**
  - vários ocorrendo no Brasil
  - internacionalmente DD4BC atacando instituições financeiras, realizando extorsão com pagamento via *bitcoin*
- ***Botnets* compostas de:**
  - *desktops*, servidores *Web*, dispositivos móveis, CPEs, CCTVs, raio X, etc.
- **Mitigação é realmente difícil**
  - técnicas de mitigação tem que levar em conta questões de privacidade e possibilidade de descarte de trafego legitimo

Malware

- **RAT e *ramsomware* em amplo uso**
- **"*Government Grade Malware for the Masses*"**
  - vazamento do *Hacking Team*, código fonte disponível para atacantes
  - código multiplataforma: "*Windows, Windows Phone, Windows Mobile, Mac OSX, iOS, Linux, Android, BlackBerry OS, and Symbian*"
- **Novos *malwares* sendo desenvolvidos**
  - difíceis de serem detectados por antivírus
  - difíceis de serem simulados em *sandboxes*
    - necessitam de condições específicas
- **Grande mercado de *zero-days***

09 Ransomware Now Gunning for Your Web Sites

NOV 15

One of the more common and destructive computer crimes to emerge over the past few years involves **ransomware** — malicious code that quietly scrambles all of the infected user's documents and files with very strong encryption. A ransom, to be paid in Bitcon, is demanded in exchange for a key to unlock the files. Well, now it appears fraudsters are developing ransomware that does the same but for Web sites — essentially holding the site's files, pages and images for ransom.

Typically, the malware is injected into Web sites via known vulnerabilities in site plugins or third-party software — such as shopping cart programs. Once on a host machine, the malware will encrypt all of the files in the "home" directories on the system, as well backup directories and most of the system folders typically associated with Web site files, images, pages, code libraries and scripts.

Fonte: http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

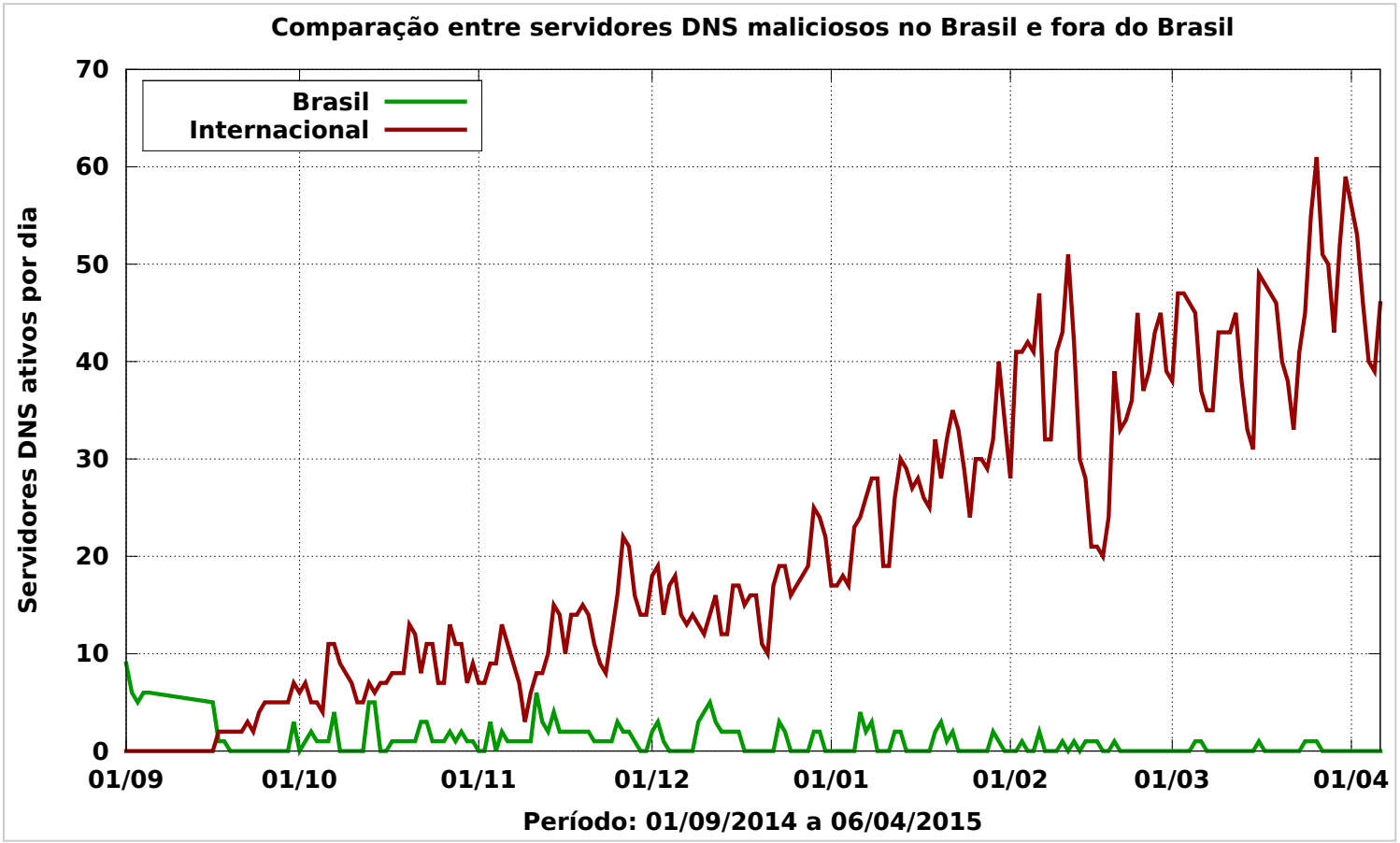
Dispositivos móveis

- **Descoberta de vulnerabilidades em ampla expansão**
  - XcodeGhost, StageFright
- **Fragmentação de versões**
  - dificuldade de atualização
- **Autenticação:**
  - esquemas convencionais não são práticos
  - necessidade de formas rápidas e seguras

Roteadores Domésticos – CPEs

- **Enorme base vulnerável**
  - sem instalação de *patches*
  - configurações padrão de fábrica com serviços com senha padrão, serviços como Telnet habilitados, etc
- **Usados para todos os tipos de ataque**
  - *botnets* para DDoS e mineração de *bitcoins*
  - comprometimento para alteração de DNS
    - pode levar a ataques:
      - *phishing*, *malware,* falsos boletos
- **Servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud***
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

Servidores DNS maliciosos ativos – Estatísticas diárias



Período:	**218 days**	**ASNs:**	**81**
Países:	**23**	**IPs:**	**423**

Fonte: CERT.br

Roteadores Domésticos – CPEs

Ataques a CPEs (*modems*, roteadores banda larga, etc)

- **comprometidos via força bruta de telnet**

```
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, status:
SUCCEEDED, login: "root", password: "root"
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "sh"
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "echo
-e \\x51\\x51"
2014-03-24 16:19:01 +0000: dlink-telnetd.pl[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: dlink-telnetd.pl[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"
```

Strings do binário baixado:

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

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

Fonte: CERT.br

Roteadores Domésticos – CPEs

Ataques a CPEs (*modems*, roteadores banda larga, etc)

- **comprometidos via força bruta de telnet**

```
2015-02-02 22:42:07 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd:
"dns --help"
2015-02-02 22:42:07 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd
response: "
Usage: dns config auto

Usage: dns config static [<primary DNS> [<secondary DNS>]]
       dns show
       dns --help
"
2015-02-02 22:42:24 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd:
"dns show"
2015-02-02 22:42:24 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd
response: "
Primary   10.1.1.1
Secondary 10.1.1.1

"
```

Fonte: CERT.br

IoT

- **Cada vez mais equipamentos/sistemas conectados**
- **Falta de cuidados de segurança**
  - no projeto, implementação e adoção
  - dificuldade de atualização de sistemas
    - lâmpadas Phillips Hue LED:
      - criptografia fraca permite descobrir senha do Wi-Fi
      - vulnerabilidades permitem controlar remotamente
    - TVs Samsung:
      - mandam o som ambiente para sede
    - TVs LG:
      - enviam nomes de arquivos, filmes e *drives* de rede
    - carros da Fiat Chrysler:
      - controle dos veículos via 3G/4G, explorando vulnerabilidades do Uconnect
    - aviões:
      - potencialmente vulneráveis via sistemas de entretenimento
    - dispositivos médicos

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

Contact Hospira

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

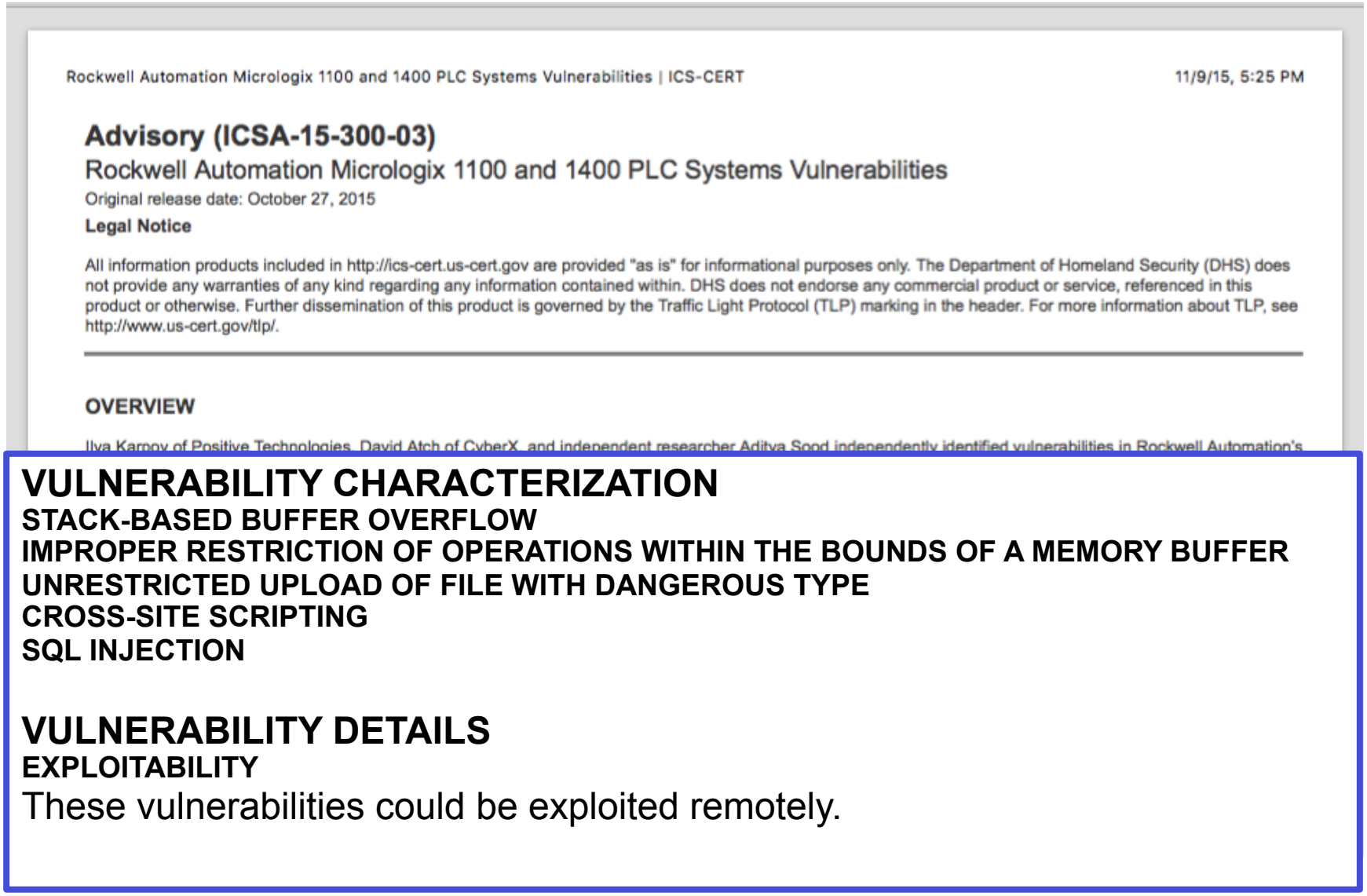
IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.



Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities | ICS-CERT 11/9/15, 5:25 PM

Advisory (ICSA-15-300-03)

Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities

Original release date: October 27, 2015

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Ilya Karpov of Positive Technologies, David Atch of CyberX, and independent researcher Aditya Sood independently identified vulnerabilities in Rockwell Automation's

VULNERABILITY CHARACTERIZATION

STACK-BASED BUFFER OVERFLOW
IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER
UNRESTRICTED UPLOAD OF FILE WITH DANGEROUS TYPE
CROSS-SITE SCRIPTING
SQL INJECTION

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

Fonte: https://ics-cert.us-cert.gov/advisories/ICSA-15-300-03

Imperva, Inc.

CCTV Botnet In Our Own Back Yard | Incapsula.com

IMPERVA INCAPSULA

PRODUCTS ENTERPRISE PARTNERS BLOG

The Incapsula Blog

Attack Details

As noted, this assault consisted of HTTP GET floods that peaked at around 20,000 RPS, with its traffic originating from roughly 900 CCTV cameras spread around the globe. Their target was a rarely-used asset of a large cloud service, catering to millions of users worldwide.

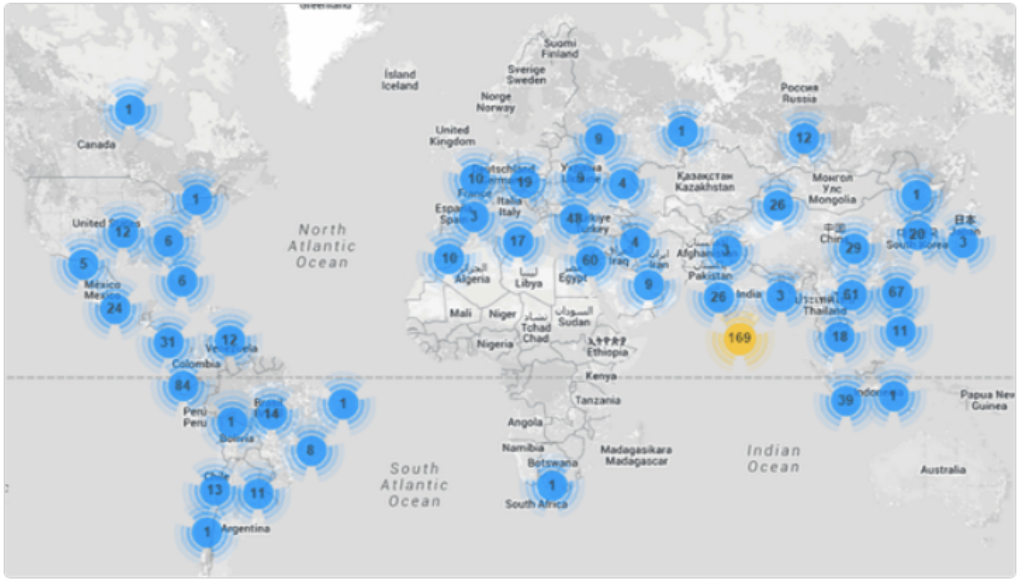


Figure 1: Geo-location of botnet devices

Fonte: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

Outros

- **Acessibilidade em s*ites***
- **Redes sociais como vetor de rápida propagação**
- **Lições aprendidas da Copa 2014**
  - apontam para desafios adicionais em 2016
  - olimpíadas/manifestações
  - alvos difusos
  - criminosos se transfiguram em “*hacktivistas*”

Desafios:
Como melhorar o cenário

cert.br nic.br cgi.br

Precisamos um ecossistema mais saudável

Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança – todos possuem um papel

- **Administradores de redes e sistemas**
  - não emanar “sujeira” de suas redes e adotar boas práticas
    - implementar BCP38 (http://bcp.nic.br/)
    - implementar gerência de porta 25
  - notificar usuários sobre infecções e indícios de comprometimento
  - fazer *hardening* das máquinas

Precisamos um ecossistema mais saudável

- **Usuários**
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções
  - usar verificação em duas etapas
- **Desenvolvedores**
  - pensar em segurança desde o início
  - pensar nos casos de ABUSO (o ambiente é HOSTIL)
- **Acadêmicos**
  - incluir conceitos de programação segura logo nos primeiros anos
  - realizar pesquisas na área
    - novos cenários necessitam de novos paradigmas

Áreas de pesquisa (1/3)

- ***Malware*:**
  - *sandbox*:
    - como estimular o *malware* a entrar em ação?
  - *SDN Rootkits: Subverting Network Operating Systems of Software-Defined Networks*
    - *18th International Symposium, RAID 2015, Kyoto, Japan, November 2–4, 2015, Proceedings*
    - *http://link.springer.com/chapter/10.1007/978-3-319-26362-5_16?no-access=true*

- **Autenticação em dispositivos móveis**
  - desafios
  - localizações recentes
  - imagens

Áreas de pesquisa (2/3)

- **Pesquisas comportamentais**
  - principalmente com crianças
  - percepção dos usuários frente aos novos modelos
  - privacidade X comodidade
  - *Symposium On Usable Privacy and Security* (SOUPS)
    - https://cups.cs.cmu.edu/soups/

- **DDoS**
  - novas técnicas de mitigação
  - maioria das técnicas acaba não bloqueando
    - na verdade efetivam o problema (auto DDoS)
  - limpeza de trafego efetiva
    - dificuldade de fazer pesquisa técnica

Áreas de pesquisa (3/3)

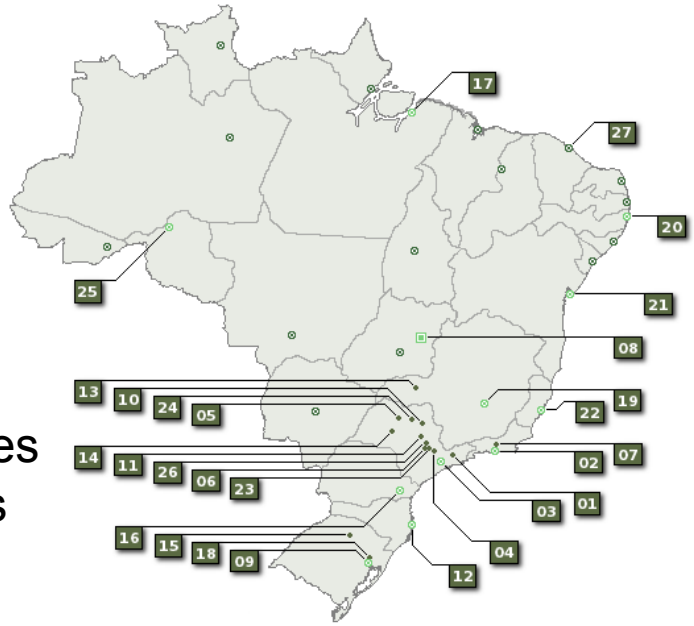
- **Outros**
  - formas de apresentar os resultados expondo vulnerabilidades
  - acessibilidade de *sites*
  - atualização de CPEs
  - auditoria de código seguro
  - *honeypots* em redes IPv6
  - propagação de informações via redes sociais

Projetos conduzidos pelo CERT.br

cert.br nic.br cgi.br

Projeto Honeypots Distribuídos

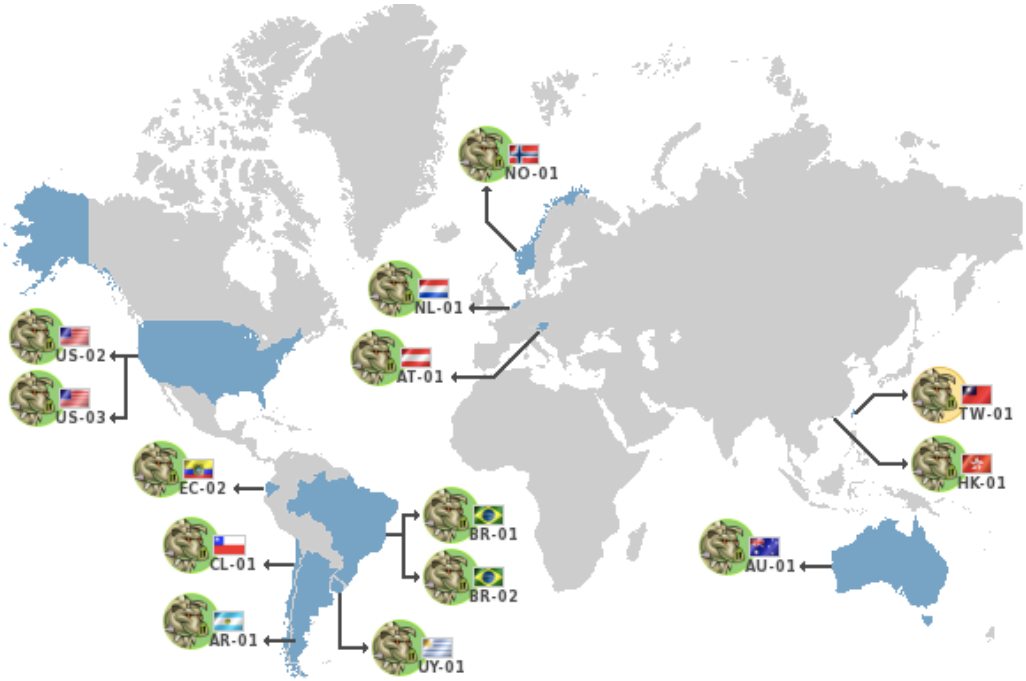
- **Foco: ataques de rede**
- **60 sensores, 22 cidades, 50 parceiros voluntários**
  - governo, provedores, áreas acadêmica, financeira e de energia
  - acordo para manter confidencialidade dos dados
- **Configuração transparente**
  - dados de produção não são capturados
- **Dados coletados:**
  - em servidor central do CERT.br
  - doados para outros CSIRTS e parceiros
  - usados para:
    - notificar redes que originaram os ataques
    - gerar estatísticas e observar tendências



http://honeytarg.cert.br/honeypots/

Projeto Spampots

- **Foco: dados relativos ao abuso de máquinas conectadas via redes de banda larga para envio de *spam***
- **Mineração de dados**
  - pesquisa em conjunto com UFMG
  - chamada de propostas realizada em 2006



14 sensores em 12 países, com apoio de:

- CSIRT UNLP (AR)
- AusCERT (AU)
- CERT.at (AT)
- CSIRT USP (BR)
- CLCERT (CL)
- CSIRT CEDIA (EC)
- HKCERT (HK)
- SurfCERT (NL)
- Shadowserver (NO eUS)
- TWCERT (TW)
- University of Alabama at Birmingham (US)
- CSIRT ANTEL (UY)

Portal para os membros do projeto Spampots

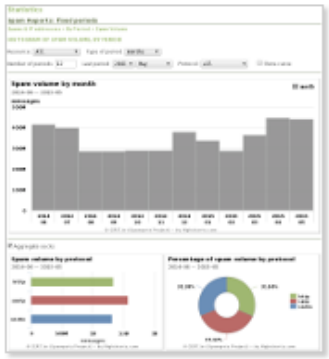
- IP addresses
- Messages per IP
- Change Over Time
  - Total
  - Country Codes
  - AS Numbers

Spampots Comparison

- By Period
  - Spam Volume
    - grid chart
  - Messages per IP
    - grid chart
- Change Over Time
  - Spams & IPs
    - grid chart

- Tables
- raw data

back



HISTOGRAM OF SPAM VOLUME, BY PERIOD

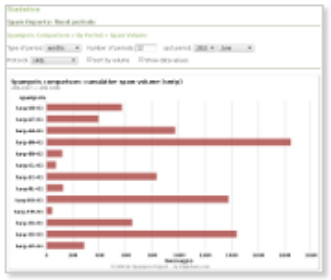
Histogram of spam volume by period, which can be months, quarters, semesters or years. Also shows the spam volume by protocol for the whole period, and corresponding percentages. It can be filtered by resource, selecting all spampots, an specific one, or a country that hosts an spampot. The histogram can also be filtered by protocol.

HISTOGRAM OF IP ADDRESSES, BY PERIOD

Histogram of IP addresses by period, which can be months, quarters, semesters or years. It can be filtered by resource, selecting all spampots, an specific one, or a country that hosts an spampot. The histogram can also be filtered by protocol.

CDF OF MESSAGES PER IP, BY PERIOD

Cumulative Distribution Function (CDF) of messages per IP address in a given period.

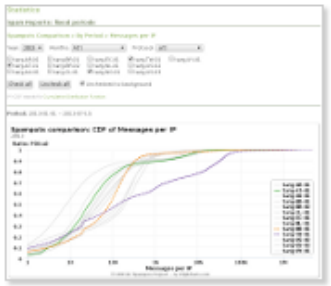


SPAM VOLUME PER SPAMPOT, BY PERIOD

Comparison of spam volume per spampot, for a given period. It can be filtered by protocol, and sorted by volume.

SPAM VOLUME PER SPAMPOT, BY PERIOD (grid chart)

Grid chart comparing the spam volume by protocol of each spampot, for a given period. The graphics displayed can be bars, columns or pie charts.



CDF OF MESSAGES PER IP PER SPAMPOT, BY PERIOD

Comparison of the cumulative distribution function (CDF) of messages per IP address by spampots, for a given period. It can be filtered by protocol.

Obs. The unchecked spampots' curves can be kept on the background, by marking the corresponding checkbox.

CDF OF MESSAGES PER IP PER SPAMPOT, BY PERIOD (grid chart)

Portal para os membros do projeto Spampots

From: 2015-06-01

To: 2015-06-17

Spampot: All

Graphs to show:
- Total
- Spampots comparison
- Country Codes
- Autonomous Systems

Region: ripencc

CC*: AD,AE,AL

ASN*: All

Top N: 5

Protocol: All

Grouped by: day

Chart options:
- SOCKS aggregated
- SMTP only
- Smooth lines
- Show markers

Submit

Defaults

Statistics

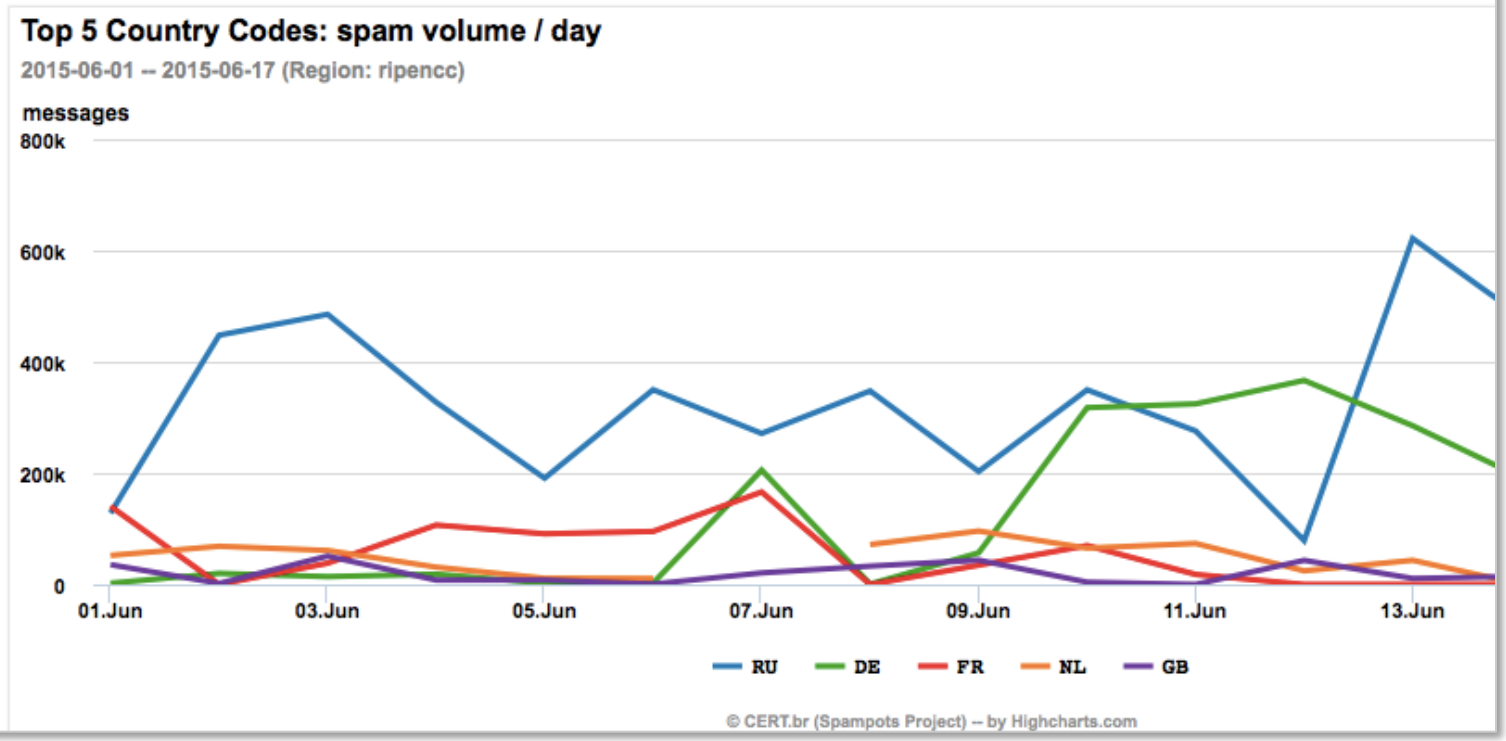
Spam Reports: database query interface

GRAPHICS

Available data: from 2012-01-01 to 2015-06-17

Selected data: from 2015-06-01 to 2015-06-17

Observed date range: from 2015-06-01 to 2015-06-17



Questões éticas

cert.br nic.br cgi.br

Ética em pesquisas de segurança (1/2)

- **Quais são os limites?**
- **É ético pesquisar:**
  - acessando dados vazados?
  - comprando produtos vendidos por meio de *spam*?
  - varrendo o endereçamento IPv4?
  - abusando da infraestrutura pública da Internet?
  - medindo a censura de *sites*?
  - testando o comportamento humano?

Ética em pesquisas de segurança (2/2)

Painéis e *papers*:

***Workshop on Ethics in Networked Systems Research* – Sigcomm 2015**

http://conferences.sigcomm.org/sigcomm/2015/netethics.php

***Will No Humans be Harmed?* – SOUPS 2012**

The argument against IRB approval for some human subjects research

Maritza Johnson, Columbia University; Michael Zimmer, University of Wisconsin-Milwaukee; Simson Garfinkel, Naval Postgraduate School; Doug Maughan, DHS Science & Technology Directorate

http://cups.cs.cmu.edu/soups/2012/program.html

***Panel on Research Ethics* – 24th Usenix Security Symposium**

Michael Bailey, University of Illinois at Urbana-Champaign; Erin Kenneally, University of California, San Diego and Elchemy, Inc.; Niels Provos, Google; Stuart Schechter, Microsoft Research

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/panel-research-ethics

Mechanical Turk is Not Anonymous

Lease, Matthew and Hullman, Jessica and Bigham, Jeffrey P. and Bernstein, Michael S. and Kim, Juho and Lasecki, Walter and Bakhshi , Saeideh and Mitra, Tanushree and Miller, Robert C.,

http://ssrn.com/abstract=2228728 or http://dx.doi.org/10.2139/ssrn.2228728

Obrigada

www.cert.br

miriam@cert.br

@certbr

10 de novembro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br