Fraudes via Internet – Estatísticas e Tendências

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

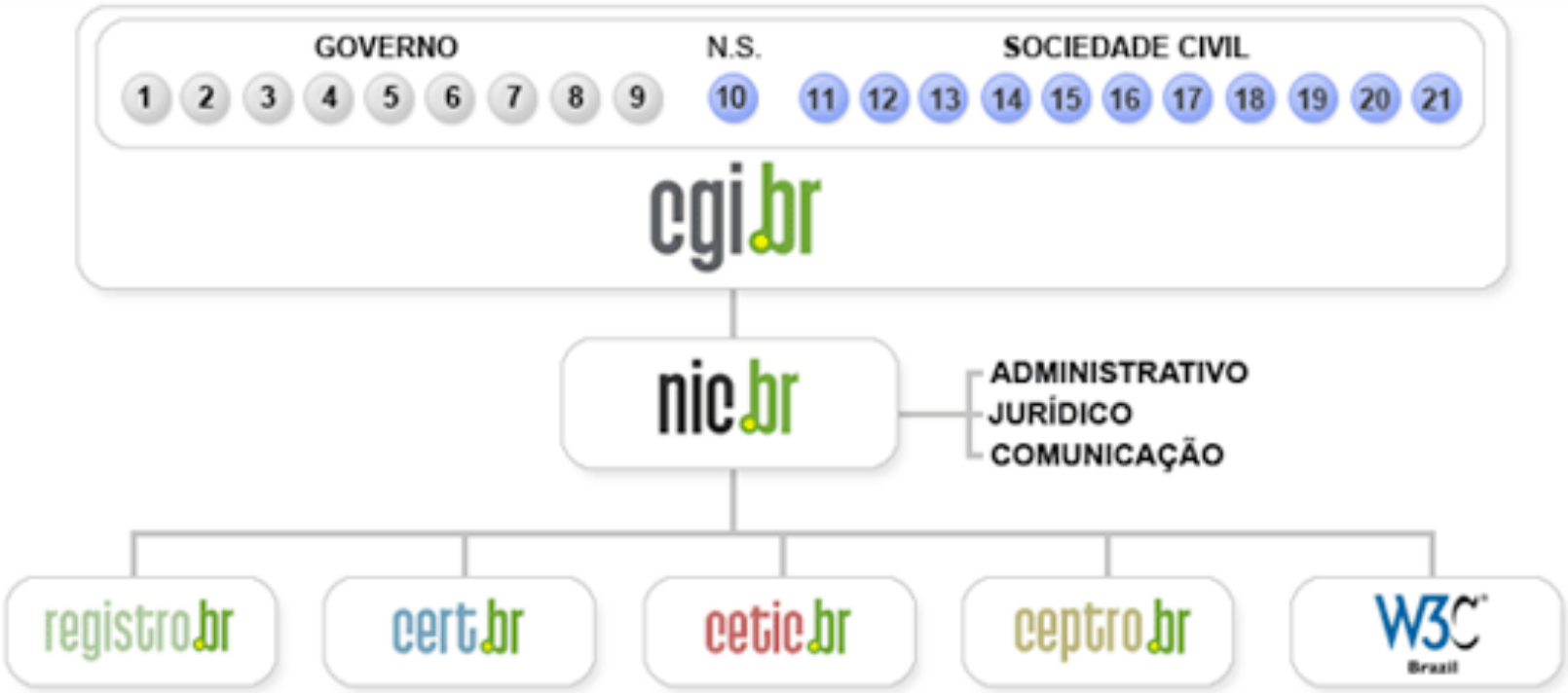
Comitê Gestor da Internet no Brasil – CGI.br

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-cg/

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

cert.br

SEI Partner Carnegie Mellon

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
– Articulação – Apoio à recuperação – Estatísticas	– Cursos – Palestras – Documentação – Reuniões	– *Honeypots* Distribuídos – SpamPots

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**

Agenda

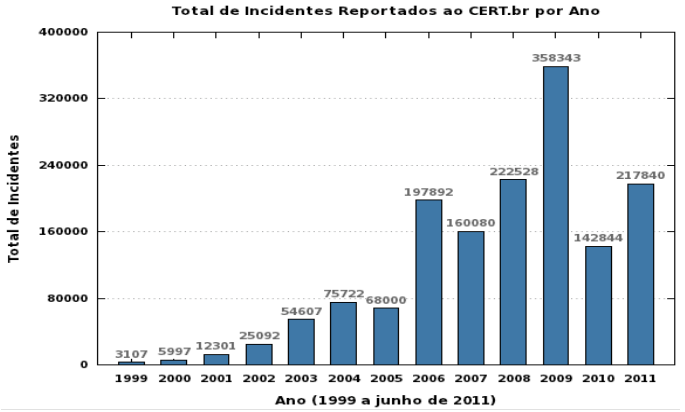
- Fontes dos dados do CERT.br
- Tipos de tentativas de fraudes financeiras mais comuns
- Estatísticas gerais das tentativas fraudes
- Estatísticas detalhadas por tipo de fraude
  - Páginas Falsas (*Phishings*)
  - Códigos Maliciosos (*Trojans*)
- Ações adotadas pelo CERT.br e por outras áreas do NIC.br
  - reativas
  - de conscientização

Fontes dos Dados Usados do CERT.br

- **Notificações voluntárias de incidentes de segurança na Internet - são a fonte de dados das estatísticas trimestrais**

  Ponto de entrada: email cert@cert.br

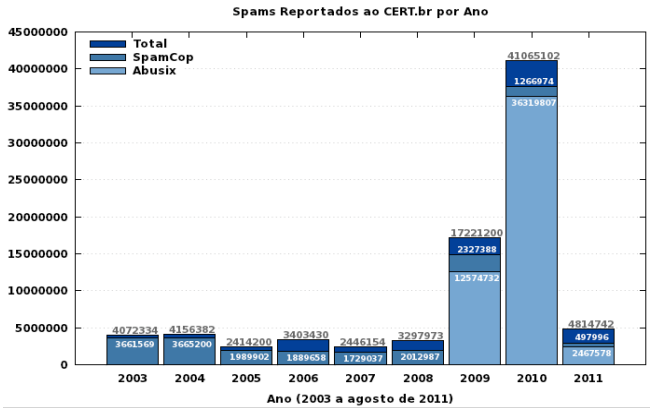
  - **2010: 885.731 *e-mails***
  - **2011 jan-nov: 938.455 *e-mails***



- ***Feeds* de ataques partindo de redes brasileiras (*Honeypots* Distribuídos , Arbor Atlas, ShadowServer, Operações anti-botnets, etc)**

Agrupados e enviados aos donos das redes, com dicas para identificação e recuperação

- **Reclamações de *Spams* que saem das redes Brasileiras - são a fonte das estatísticas de *spam* no Brasil**
  - **2011 (jan-nov): 5.914.061 reclamações**

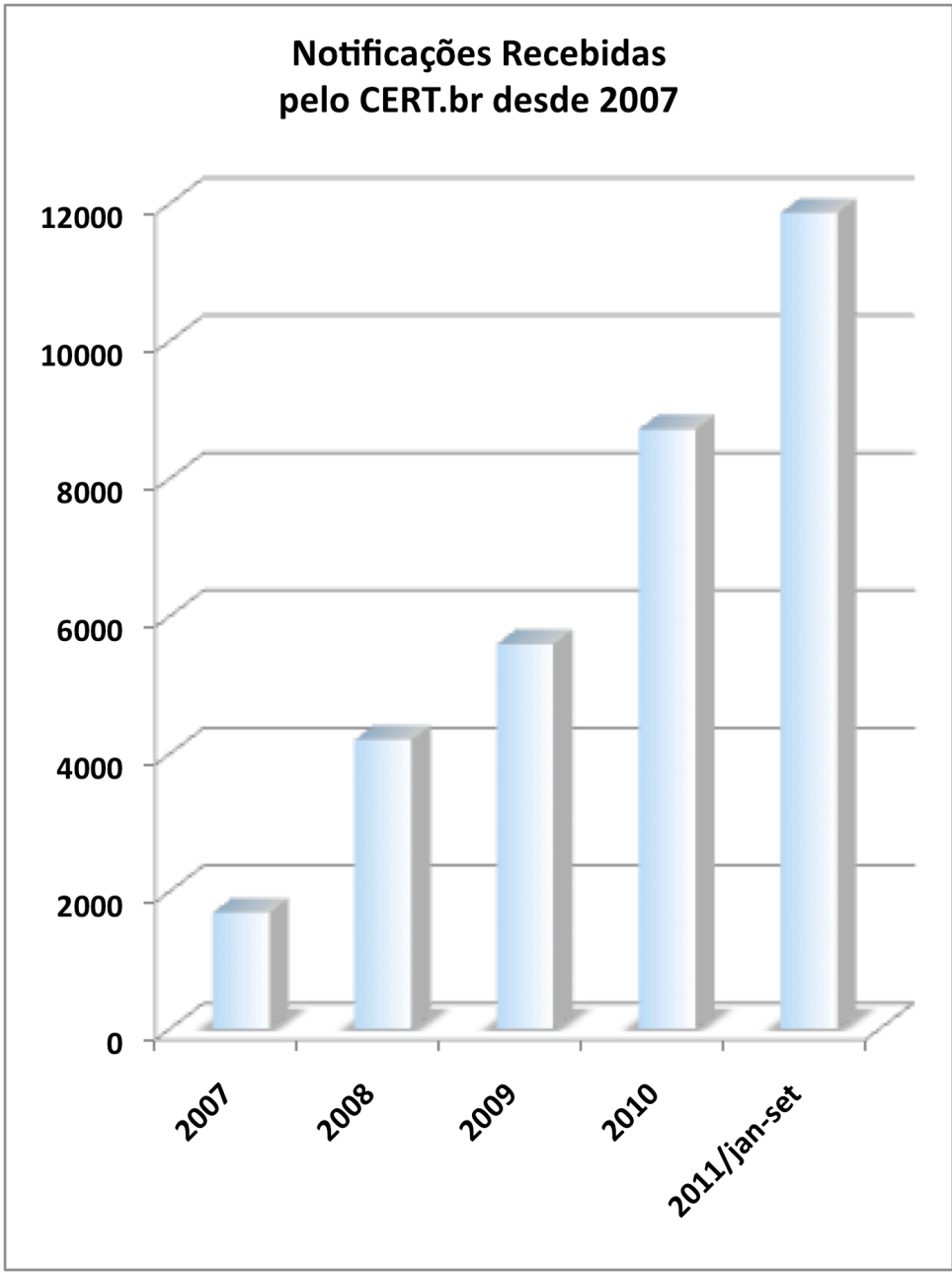


Situação dos Ataques a Usuários Finais

- **Prevalência no uso de códigos maliciosos**
  - **Diversos fins: fraudes financeiras, uso em negação de serviços (DDoS), furto de dados (*logins* de: *e-mail*, redes sociais, *windows live*, hospedagem de *sites*, consulta ao Serasa, etc)**
  - **Meios de propagação**
    - ***Spams* com temas variados e com *links* para os códigos maliciosos (por *e-mail*, redes sociais, twitter, serviços de mensagens)**
    - ***Drive-by downloads* intensamente utilizados – via códigos JavaScript e ActiveX inseridos em páginas vulneráveis, inclusive de grandes *sites***
    - **Vulnerabilidades nos sistemas operacionais e aplicativos (via PDFs e outros arquivos maliciosos)**
- **Páginas falsas de serviços variados, principalmente financeiros**
  - **em geral em combinação com algum tipo de código malicioso**
- **Códigos maliciosos para *Smartphones* e *Tablets***

Situação dos Ataques a Serviços *Web*

- **A maioria das quebras de segurança nos serviços "Web 2.0" são por falhas de programação**
  - **falta de validação de entrada e checagem de erros**
  - **uso de pacotes prontos vulneráveis**
  - **falta de atualização dos sistemas e dos pacotes**
- **Objetivos**
  - **hospedar códigos maliciosos e páginas falsas (*phishing*)**
  - **incluir o servidor em uma *botnet* e usá-lo para negações de serviço**



Obs.: **Não** são estatísticas de desfigurações *(defacements)*, são ataques a serviços *web* em geral, incluindo SQL Injection, XSS, etc

Tentativas de Fraude Tratadas pelo CERT.br

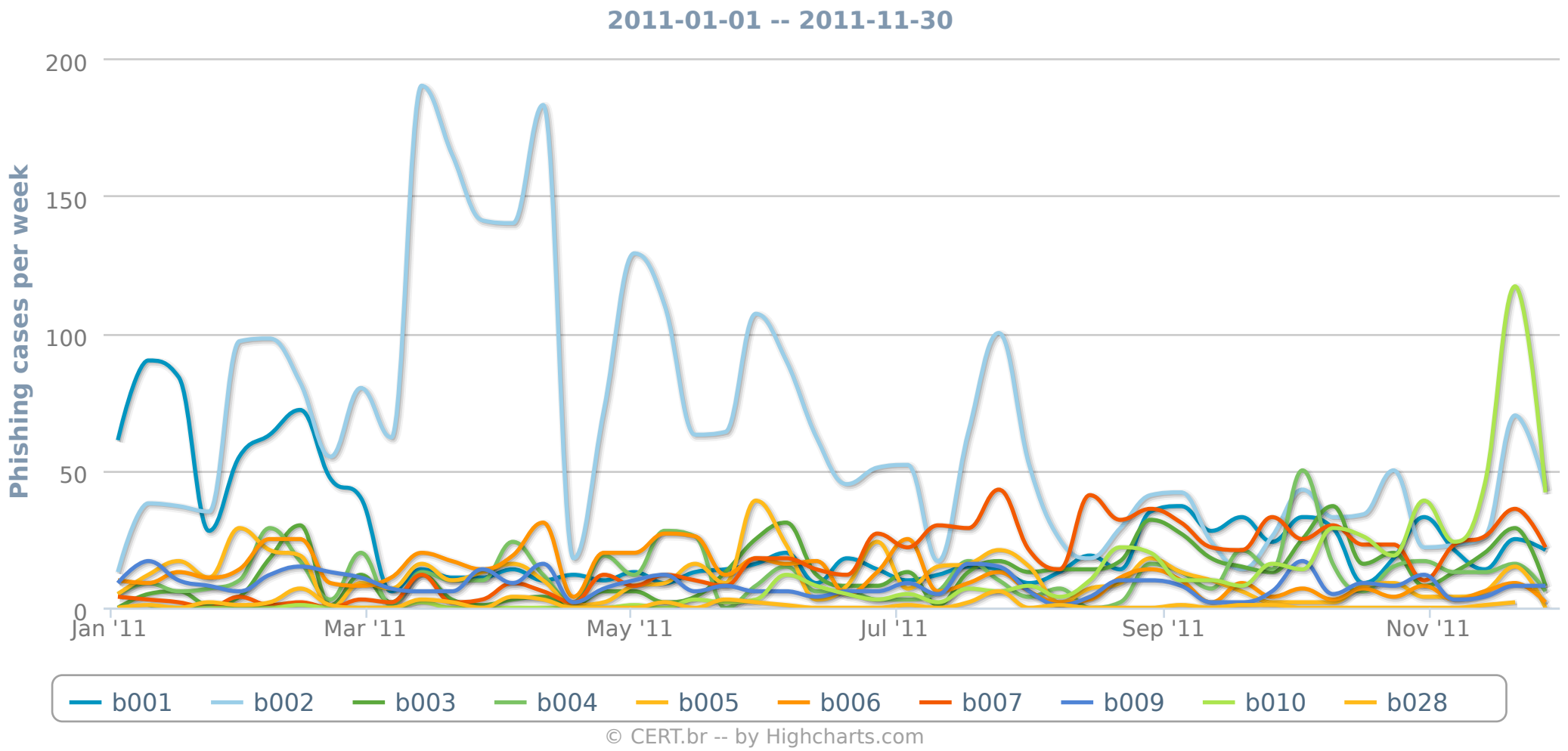
Página Falsas (Phishing)	2010	2011[A]
Número Total de Casos Tratados	7.959	11.659
Casos Envolvendo Instituições Brasileiras	***5.814***	***8.662***
Casos Envolvendo Instituições Internacionais	***2.145***	***2.997***
Países em que o conteúdo estava hospedado	70	84
Redes distintas (CIDRs)	1.099	1.315
Endereços IP envolvidos	3.496	4.754
Nomes de domínio utilizados	4.790	6.780

Códigos Maliciosos (*Trojans*)	2010	2011[B]
Número Total de Casos Tratados	10.181	8.777
Códigos maliciosos únicos	5.333	3.166
Países em que o conteúdo estava hospedado	72	64
Redes distintas (CIDRs)	1.022	955
Endereços IP envolvidos	2.553	1.939
Nomes de domínio utilizados	3.317	2.112

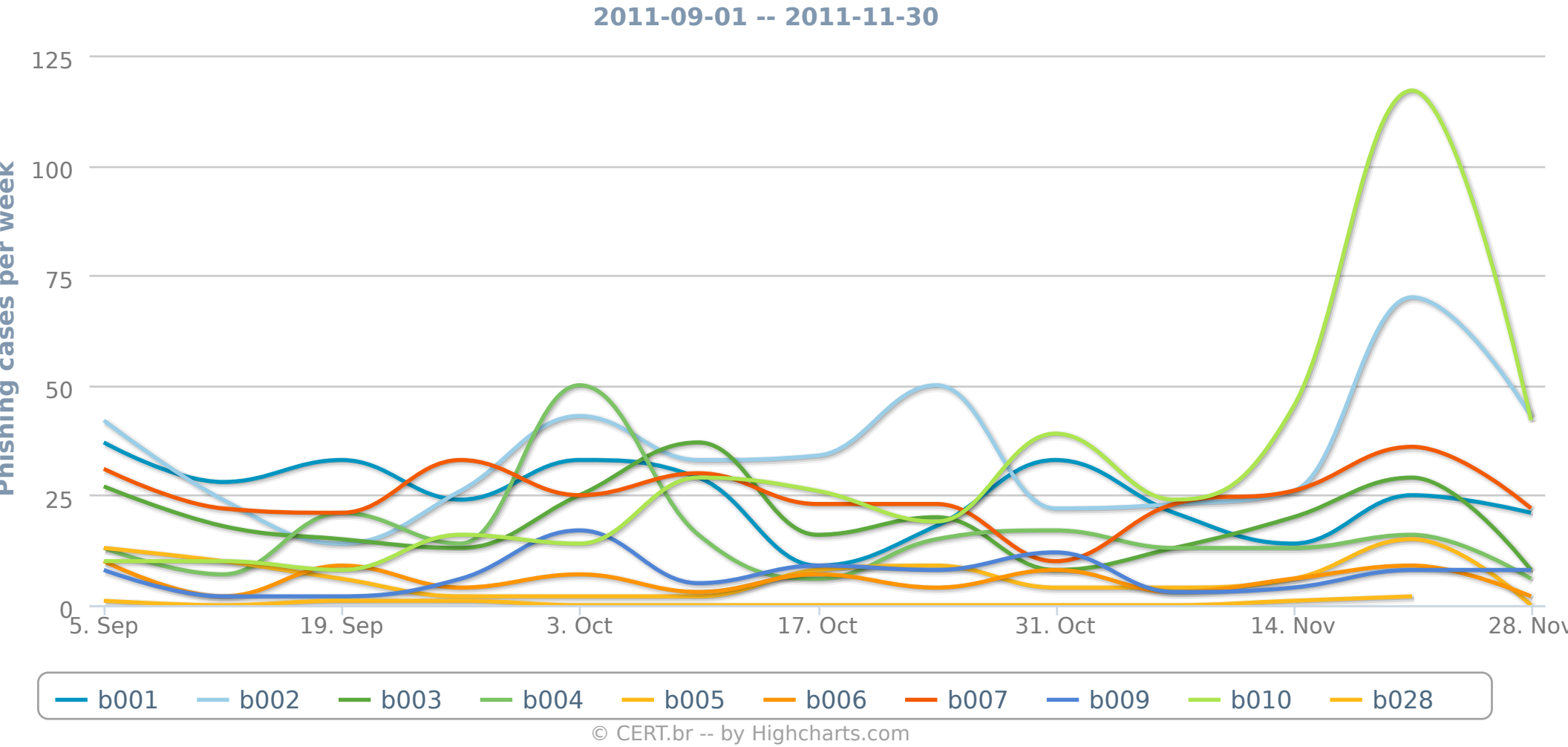
[A] Os dados de *phishings* em 2011 são referentes ao período de janeiro a novembro
[B] Os dados de *trojans* em 2011 são referentes ao período de janeiro a outubro

Estatísticas Específicas – Páginas Falsas (*Phishings*)

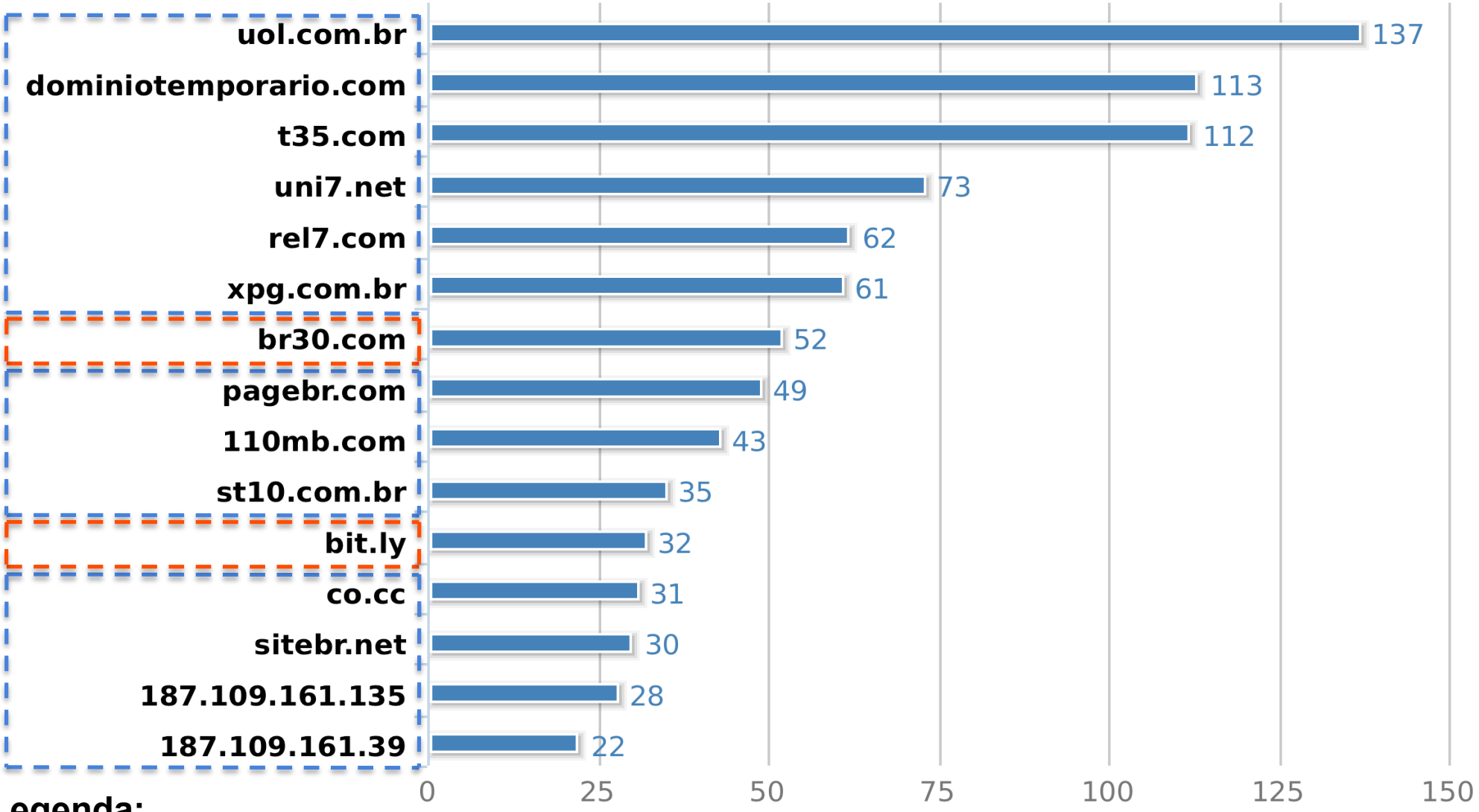
Casos de Phishing ao Longo do Tempo – 2011, casos por semana



Casos de Phishing ao Longo do Tempo – Setembro-Novembro/2011



2011 – Domínios mais Usados

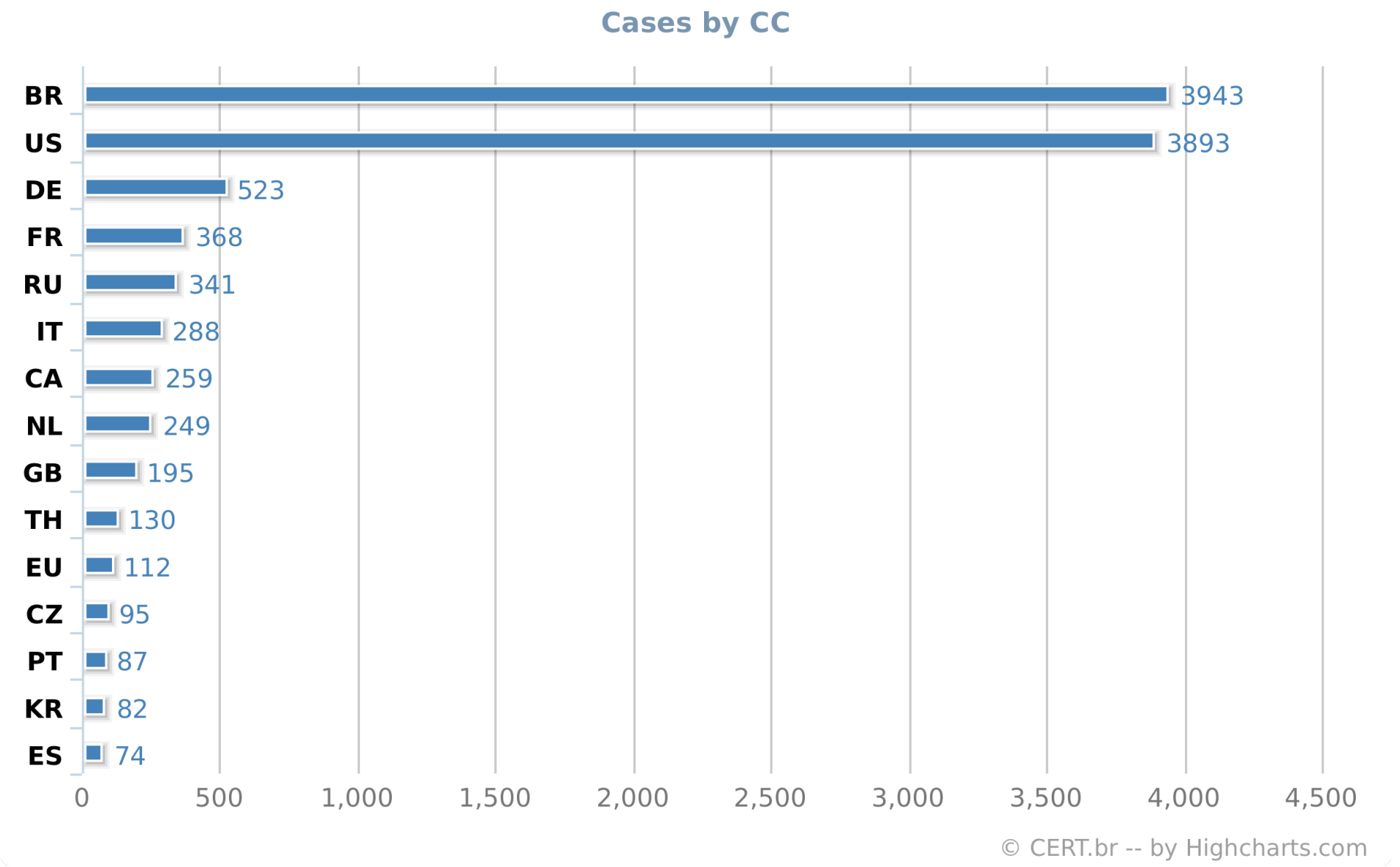


Legenda:

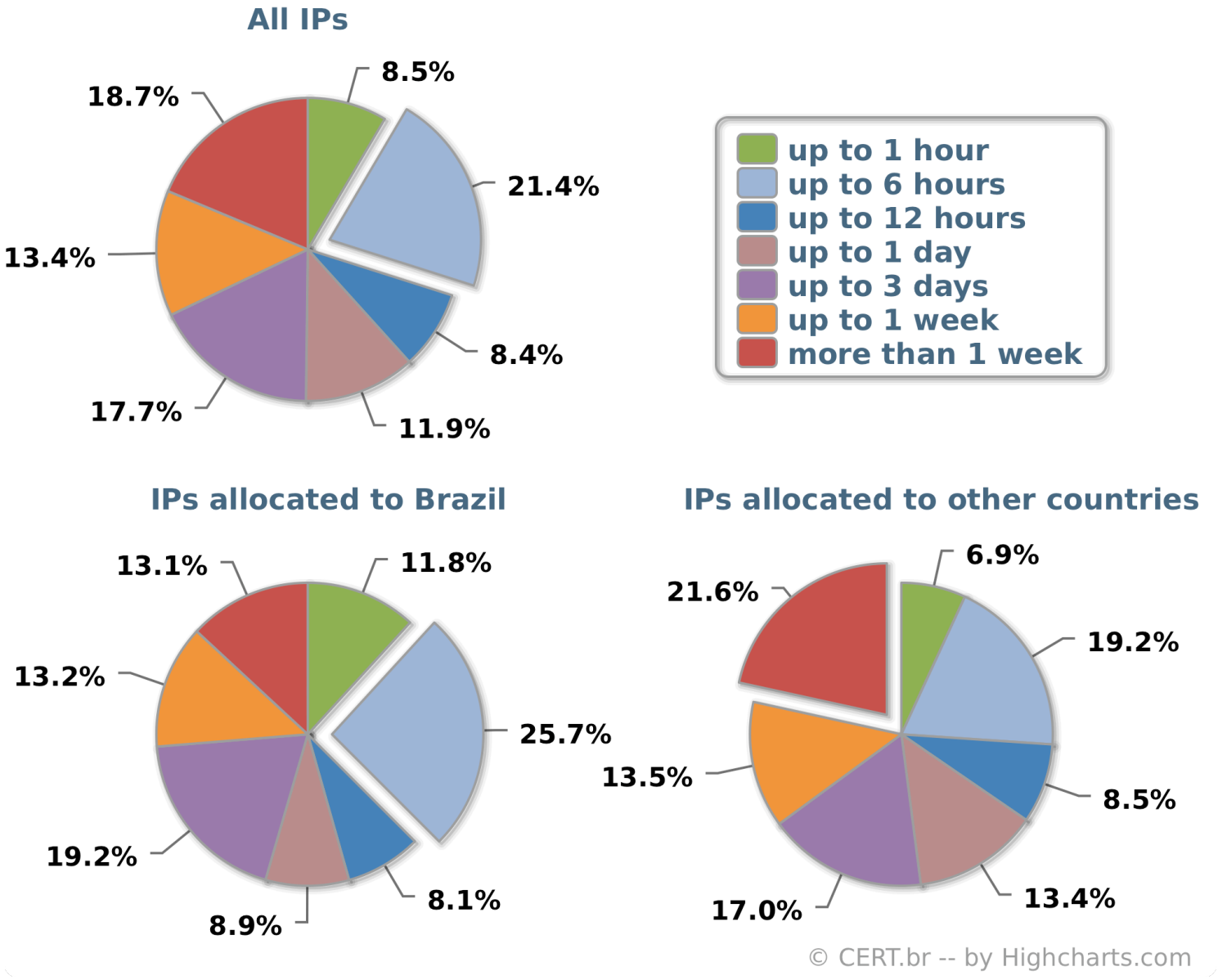
empresa de hospedagem (paga ou gratuita)

serviço de redireção de sites e/ou encurtador de URL

Países de Alocação dos IPs que Hospedam Phishing

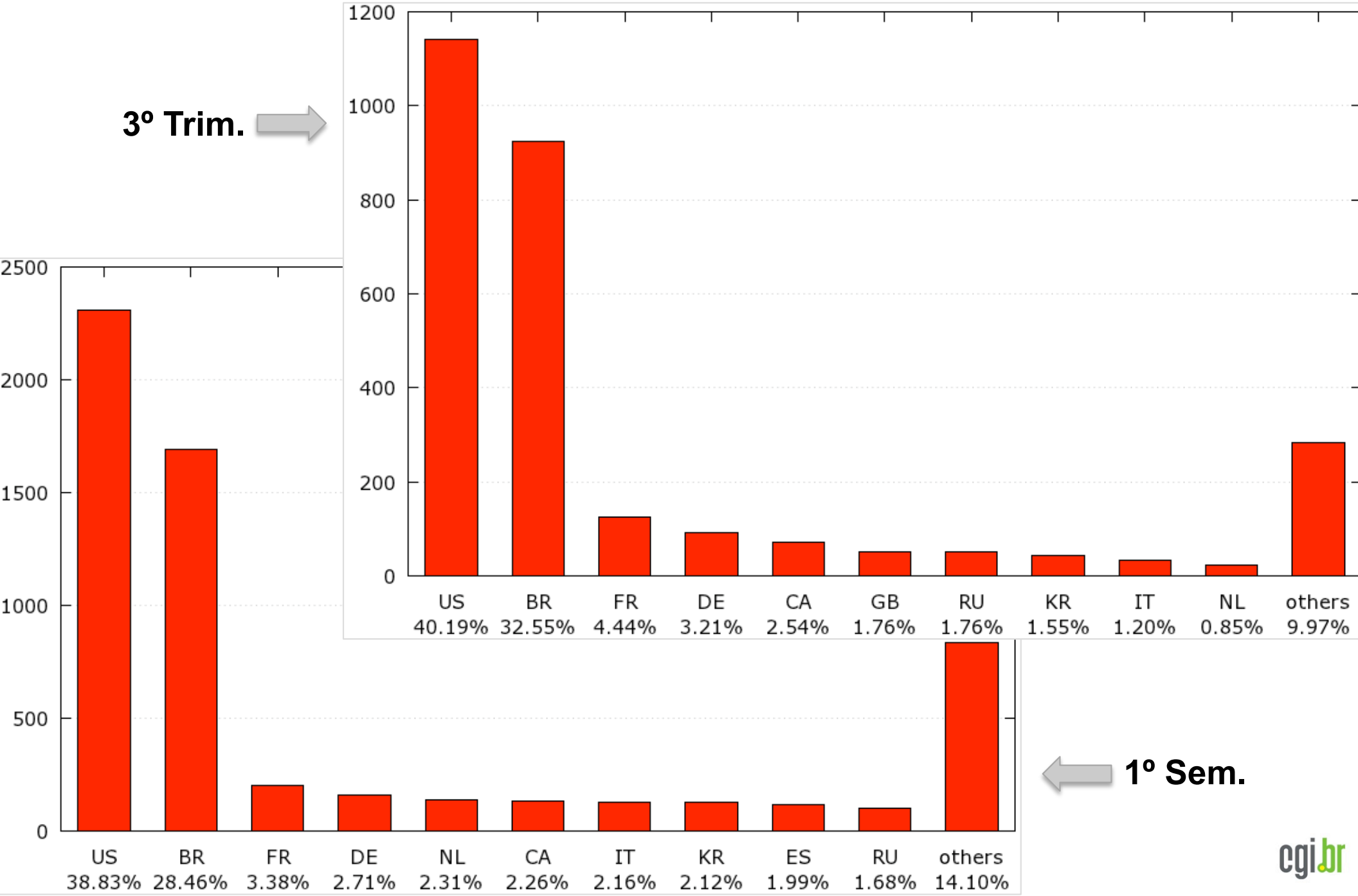


2011 – Tempo Médio no Ar – por Localização do IP

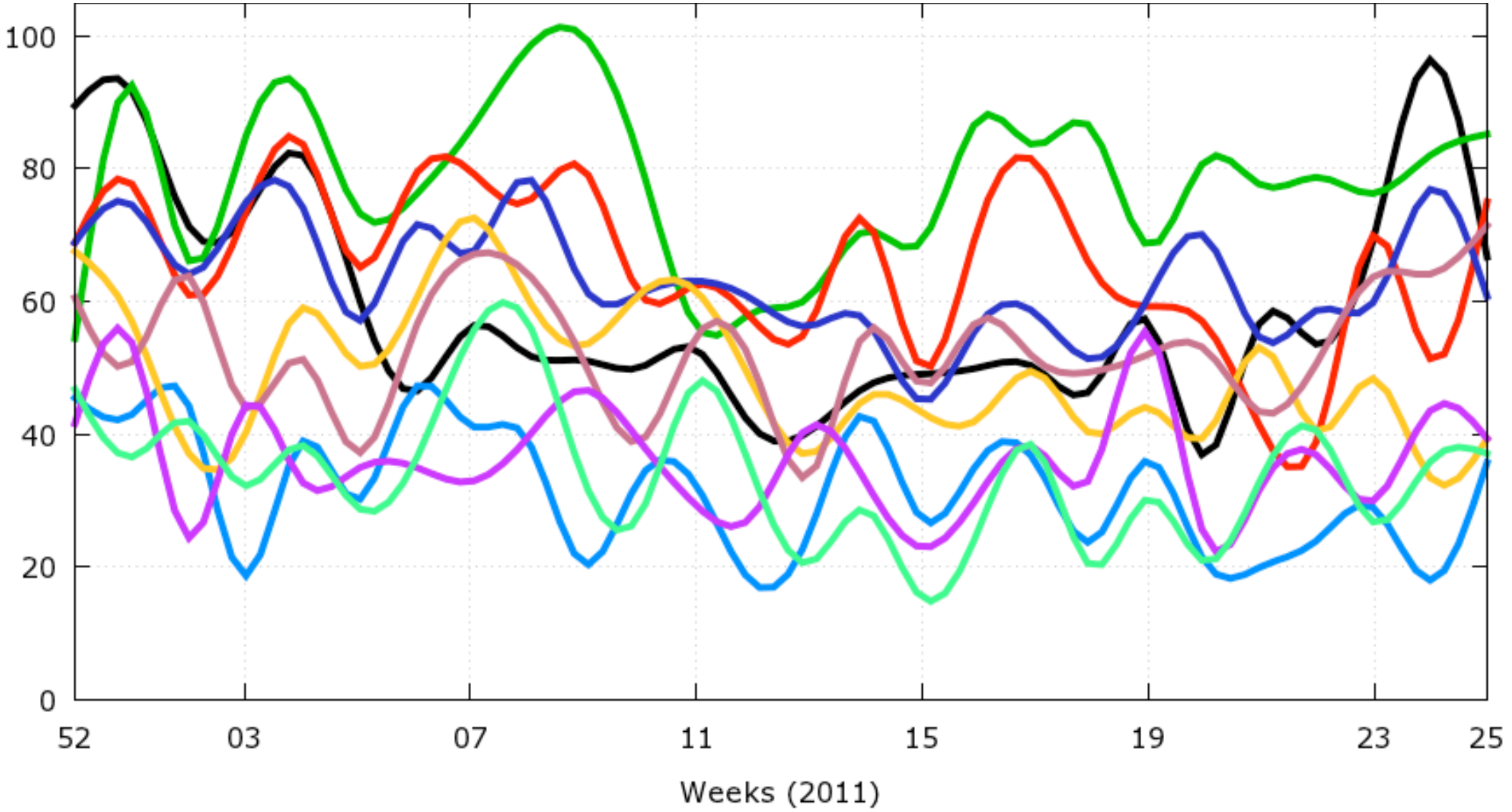


Estatísticas Específicas – Códigos Maliciosos (*Trojans*)

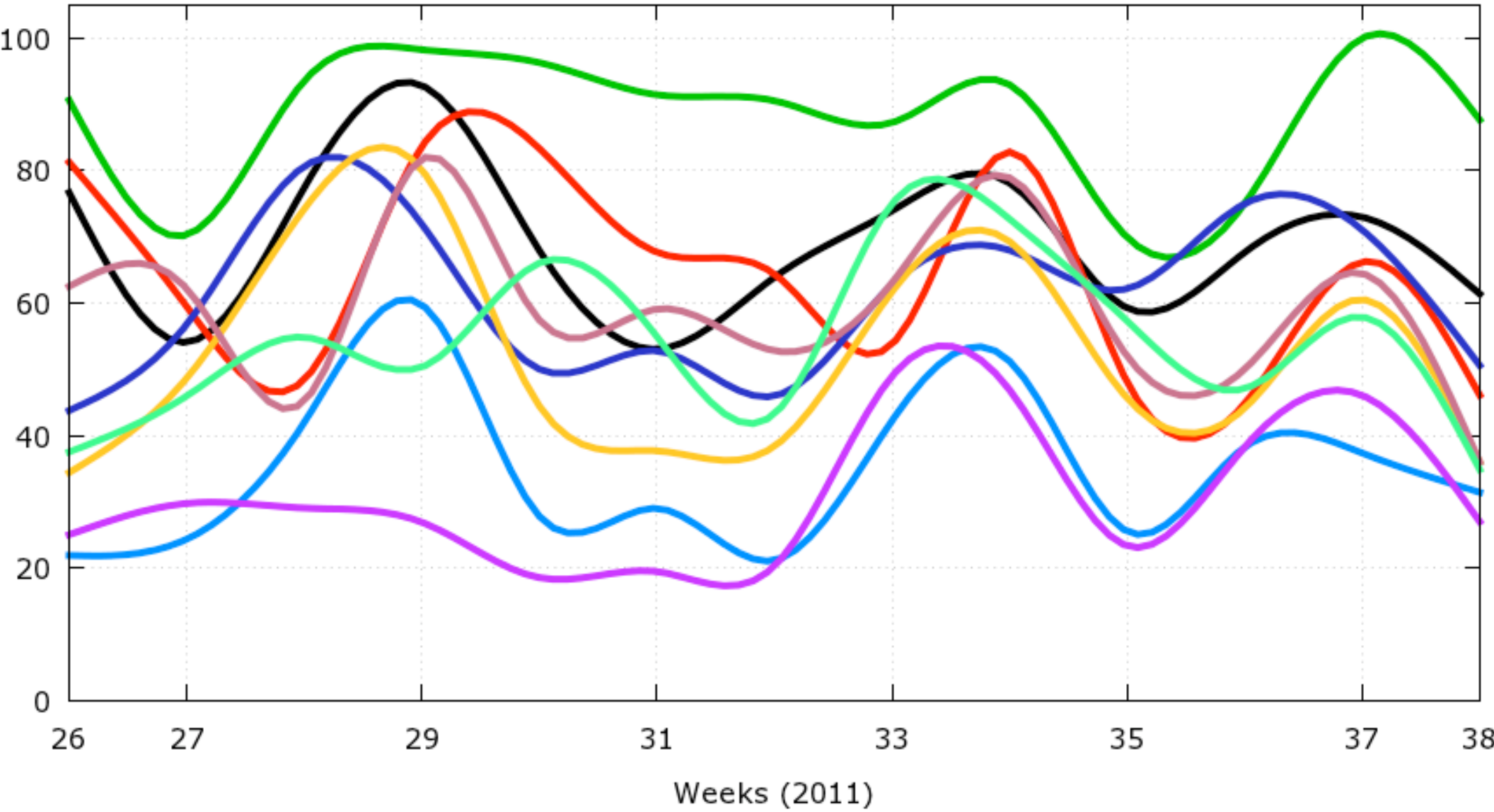
Países de Alocação dos IPs



1º Sem. – Eficiência dos Antivírus no Momento da Primeira Notificação de um Novo Malware



3º Trim. – Eficiência dos Antivírus no Momento da Primeira Notificação de um Novo Malware



Ações do CERT.br e de Outras Áreas do NIC.br

Ações do CERT.br nos Casos de Tentativas de Fraude

Foco na redução do número de vítimas de fraudes:

- **redução do tempo *online***
- **envio de informações para as ferramentas usadas pelos usuários**

Ações nos casos *phishing*

- **Notificar as redes que estão hospedando o *phishing* para que o conteúdo seja removido**
- **Enviar as URLs de *phishing* para os fabricantes de navegadores e serviços de proteção:**
  - **Firefox**
  - **Internet Explorer**
  - **Yahoo!**
  - **Trendmicro**
  - **UOL**

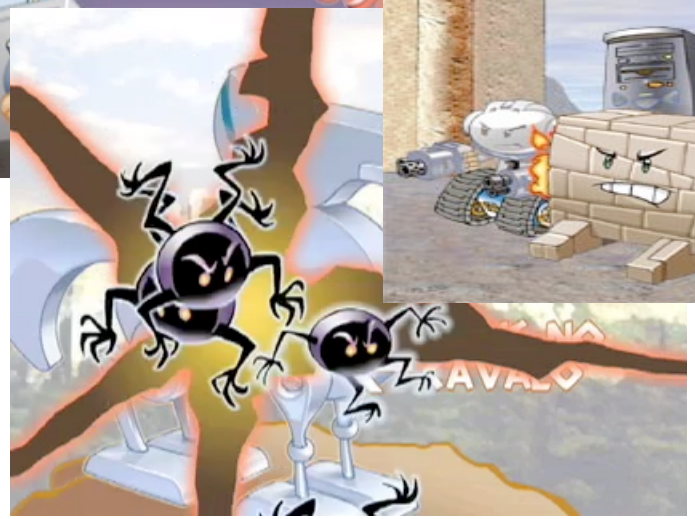
Ações nos casos de *trojans*

- **Notificar as redes que estão hospedando o *trojan* para que ele seja removido**
- **Enviar o exemplar para fabricantes de antivírus**
  - **mais de 35**
- **Enviar o código para as instituições afetadas**
  - **identificação das técnicas**
  - **auxílio a investigações sendo conduzidas**

Produção de Material Gratuito para Educação sobre Riscos e Proteção na Internet

- Cartilha de Segurança para Internet
- Site Antispam.br
- Vídeos Educacionais
- InternetSegura.br

INTERNET SEGURA.BR



Proteção da Infra-Estrutura Crítica de Internet

- **Manutenção da Hora Oficial do Brasil para sincronia de tempo em computadores – NTP.br**
- **Manutenção dos Pontos de Troca de Tráfego nas áreas metropolitanas – PTT.br**
- **Manutenção de espelhos de 3 servidores raiz DNS no Brasil**
- **DNSSEC no .br**
  - **Brasil foi o segundo ccTLD a adotar DNSSEC**
  - **Hoje temos todo o .br com possibilidade de uso de DNSSEC**
  - **Treinamento gratuito online ou presencial**
  - **.jus.br, .leg.br e .b.br só permitem domínios com DNSSEC**
- **Estímulo à segurança nos protocolos de roteamento**
  - **Segurança de BGP e RPKI em discussão pelos RIRs e no IETF**

Obs.: LACNIC é o RIR (Registro de Endereços da Internet) para a América Latina e o Caribe.
Para as demais regiões há: AfriNIC (África), APNIC (Ásia Pacífico), ARIN (América do Norte) e RIPE NCC (Europa e Oriente Médio).

Informações de Contato

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/

Cristine Hoepers
cristine@cert.br