# Ameaças Recentes, Tendências e Desafios para a Melhora do Cenário

**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

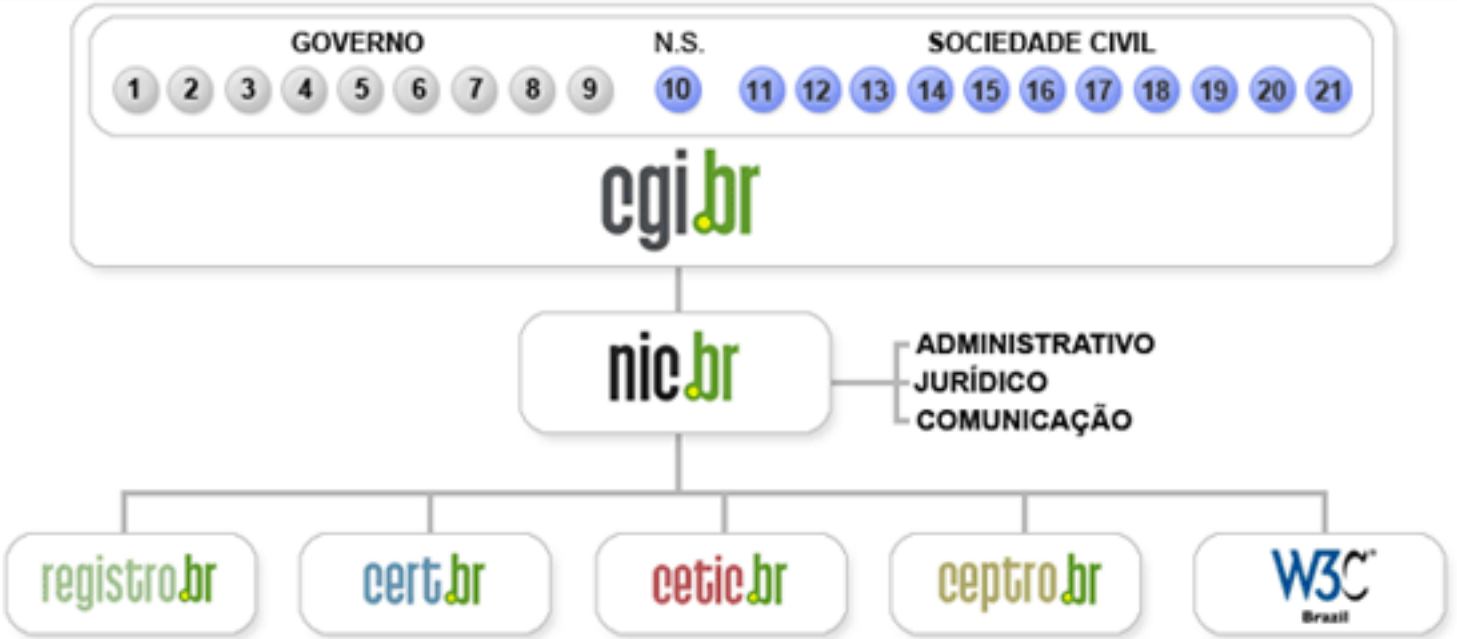
# Comitê Gestor da Internet no Brasil – CGI.br

**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;**

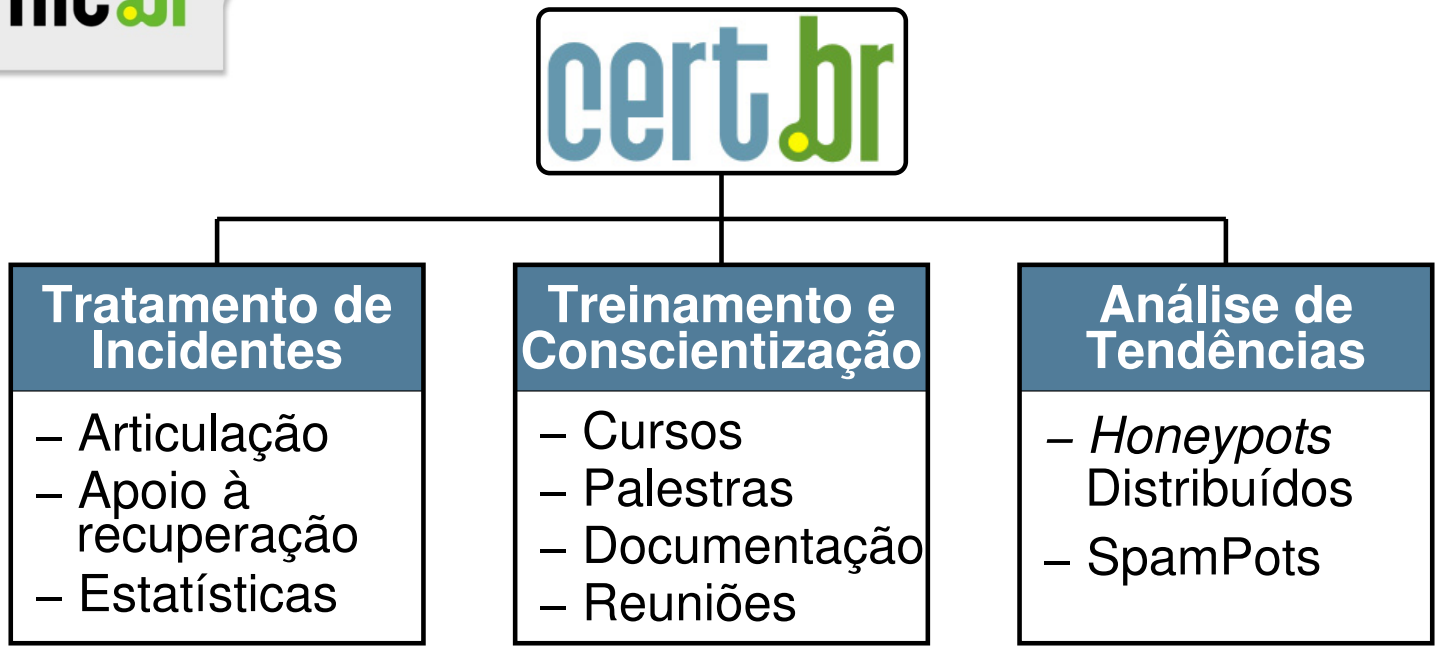
http://www.cgi.br/sobre-cg/

# 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




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/

# Agenda

- Tendências e novos vetores de ataque
- Desafios para a melhora do cenário
- Considerações finais

# Tendências e
# Novos Vetores de Ataque

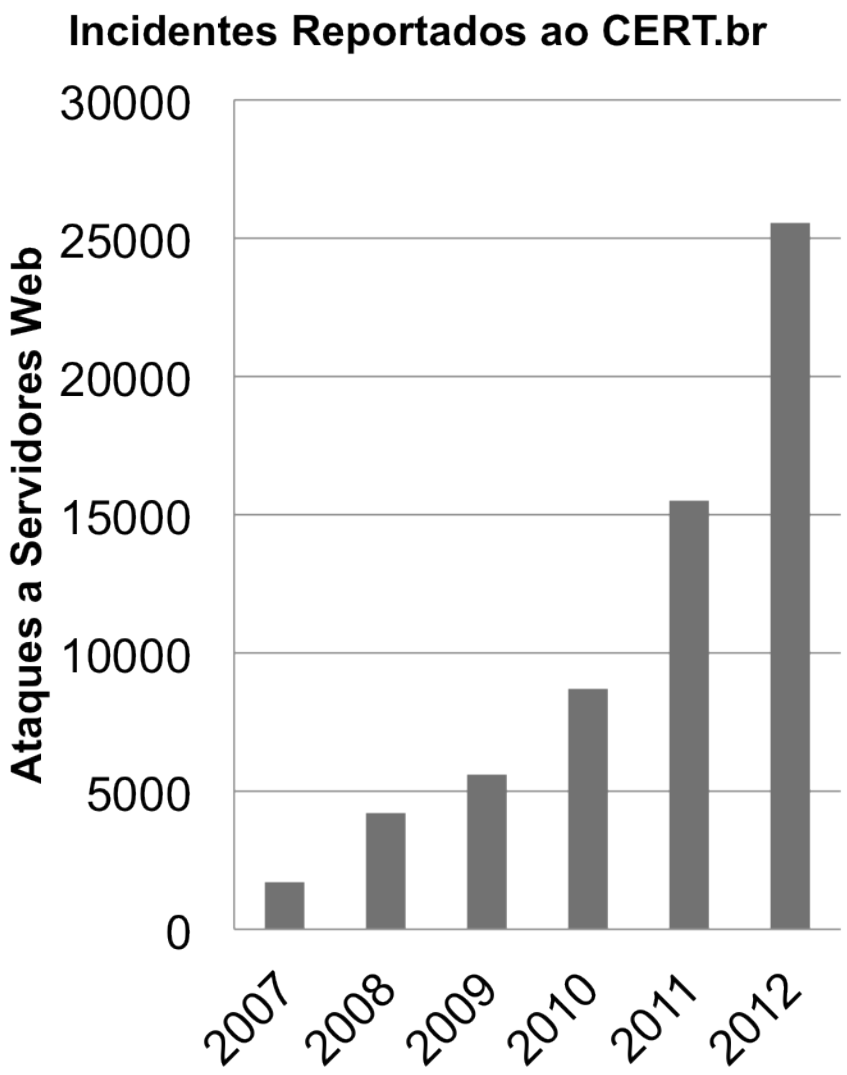
# Ataques comuns que devem continuar

- **Contra usuários finais (domésticos e corporativos)**
  - **fraudes, *phishing*, *bots*, *spyware*, etc**
  - **APTs (*Advanced Persistent Threats*)**
  - ***botnets* utilizadas para todos os fins**
- **De força bruta contra serviços de rede**
  - **SSH, FTP, Telnet, VNC, etc**
- **Contra a infraestrutura crítica da Internet**
  - **ataques contra servidores DNS**
  - **contra protocolos de roteamento como o BGP**
- **DDoS**
  - **ataques de reflexão (DRDoS) tendem a aumentar (Ex.: ataques ao SpamHaus, que chegaram a 300Gbps)**

# Ataques com rápido crescimento nos últimos anos (1/2)

## Ataques a servidores Web

- **Muitas vulnerabilidades de *Software***
  - ***softwares* de CMS desatualizados**
  - **uso de pacotes prontos**
  - **falta de atualização dos sistemas operacionais**
  - **muitas falhas de programação:**
    - **falta de validação de entrada**
    - **falta de checagem de erros**
  - **exploração automatizada**
    - **Ex.: *botnet* Brobot**



# Ataques com rápido crescimento nos últimos anos (2/2)

## Redes Sociais

- *malware* e engenharia social
- contas sequestradas, especialmente agências de notícia e personalidades

## Dispositivos móveis

- maior parte dos ataques hoje são *apps* maliciosos
- exploração de vulnerabilidades já começou

## Roteadores, modems banda larga, bases *wifi*, etc

- força bruta
- já explorados por *botnets* (Ex.: Aidra)

## *Browsers*

- *exploits*, *botnets*, etc

# Facilitadores para esse cenário

## Crescentes Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos são conectados à Internet
  - controle de infrasestruturas críticas
  - sistemas de e-gov
  - bases de dados (“*big data*”)
  - dados médicos

## Fragilidades dos Usuários Corporativos e Domésticos

- Internet passou a fazer parte do dia-a-dia
- Usuários não são especialistas
- Mais fáceis de atacar
- Grande base
  - de dispositivos vulneráveis
  - com banda disponível
- Possuem dados de valor
  - para o crime organizado (e-mails, cartões, senhas)
  - para espionagem
- Dispositivos podem ser usados para outros ataques
  - *botnets*

# Reais Causas dos Problemas

**Cenário atual é reflexo direto de**

- **Aumento da complexidade dos sistemas**
- **Falta de profissionais capacitados para desenvolver e implantar sistemas com requisitos de segurança**
- ***Softwares* com muitas vulnerabilidades**
- **Pressão econômica para lançar, mesmo com problemas**
- **É uma questão de "*Economics and Security*" http://www.cl.cam.ac.uk/~rja14/econsec.html**

**Os criminosos estão apenas migrando para onde os negócios estão**

# Desafios para a Melhora do Cenário como um Todo

# São necessários novos métodos de detecção

**Foco atual do mercado é no que entra em uma rede ou no que conhecidamente é malicioso:**

- **IDS / IPS**
- ***Firewall***
- **Antivírus**

**Foco precisa ser no que sai ou no tráfego interno:**

**"*Extrusion Detection*"**

- ***Flows***
- ***Honeypots***
- ***Passive* DNS**
- **Notificações de incidentes**
- ***Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)**

# Resiliência da Infraestrutura Crítica de Internet

**Contínuo investimento em:**

- **Pontos de Troca de Tráfego (Ex.: PTT.br)**
- **Sistemas de redundância e *mirrors* de DNS**
- **Adoção de DNSSEC**
  - **Novos protocolos, como DANE, em estudo**
- **Alternativas ou melhorias ao sistema atual de certificados digitai**
- **Segurança na infraestrutura de roteamento**
  - **Roteamento dinâmico fuciona por confiança nos anúncios**
  - **Em implantação o uso de RPKI e S-BGP**
  - **Em resumo: tabelas de rotas passam a ser assinadas e publicadas somente pela fonte legítima**

# Proteção dos Usuários Finais

**Administração dos sistemas para usuários finais precisa ser menos complexa – mudança total de paradigma de uso da tecnologia**

**Provedores de acesso e serviço, operadoras e administradores de redes em geral precisam ser mais pró-ativos para combater *botnets***

- **RFC 6561: Recommendations for the Remediation of Bots in ISP Networks – exemplos:**
  - **iCODE – Austrália**
  - **Botfrei.de – Alemanha**
  - **Irish Anti-Botnet Initiative (Botfree.ie) – Irlanda**
  - **Cyber Clean Center (CCC) – Japão**
  - **Cyber Curing System / e-Call Center 118 – Coréia**
  - **Anti-Botnet Working Group – Holanda**
  - **Abuse Information Exchange – Holanda**
  - **Autoreporter – Finlândia**
  - **U.S. Anti-Bot Code of Conduct (ABCs) for ISPs – EUA**
  - **Malware Free Switzerland – Suíça**
  - **Advanced Cyber Defence Centre / Botfree.eu – União Europeia**

# Maturidade da Indústria de *Software*

- **O processo de desenvolvimento de qualquer *software* deve incluir sempre:**
  - **Levantamento de requisitos de segurança**
  - **Testes que incluam casos de abuso**

    **(e não somente casos de uso)**

- **Desenvolvimento seguro de *software* deve se tornar parte da formação de projetistas e programadores**
  - **Desde a primeira disciplina de programação e permeado em todas as disciplinas**

# Qualificação Profissional

- **Falta pessoal para lidar com redes, segurança e tratamento de incidentes em IPv4**
  - **A falta de pessoal com essas habilidades em IPv6 é ainda mais preocupante**
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas práticas**
  - **Quantas instituições realmente implementam tecnologias com base em uma análise de risco?**
  - **Ir além do "*compliance*"**

# Considerações Finais

**Segurança é a "bola da vez" e muitas discussões serão intensificadas**

- **Segurança x Privacidade x Controle**
- **Neutralidade**
- **Governança da Internet**
- **Legislação**

# Perguntas?

**Cristine Hoepers**
cristine@cert.br

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