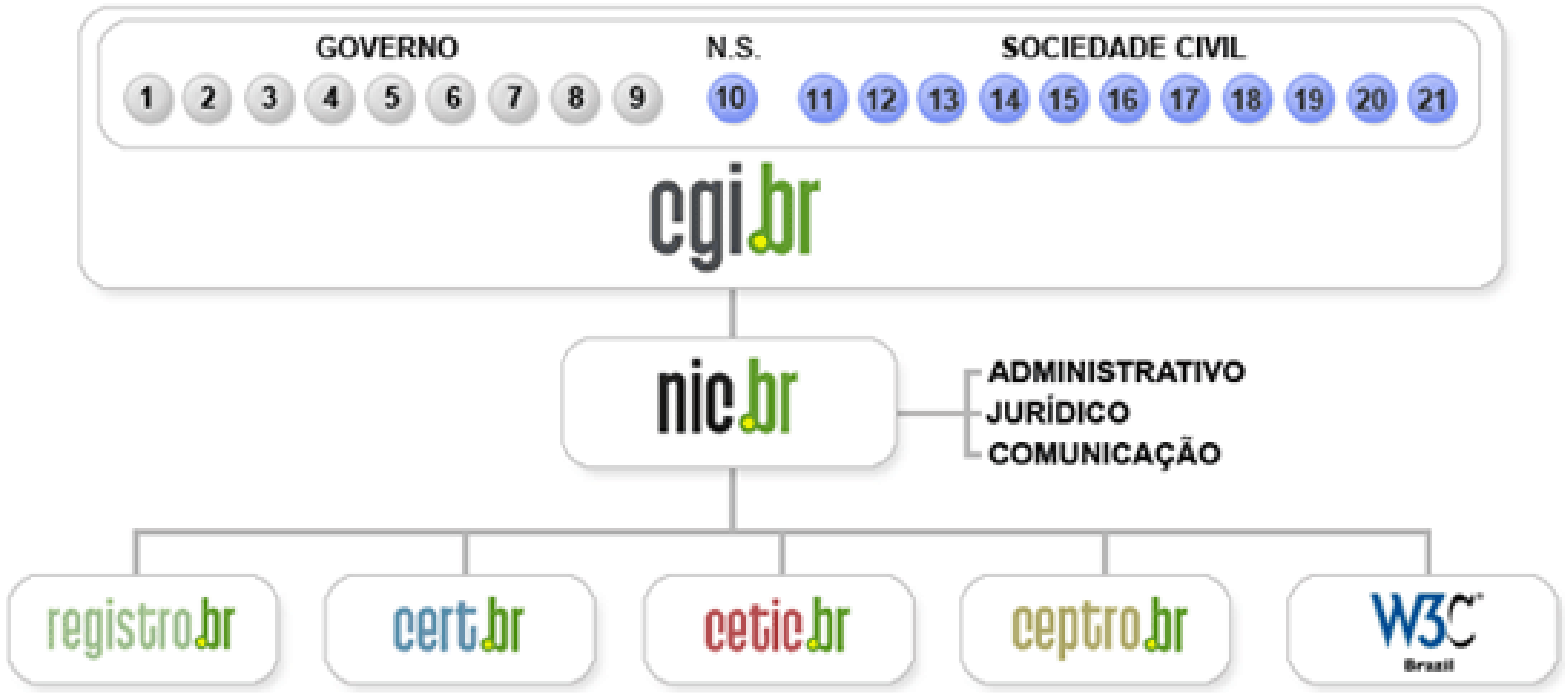
Tratamento de Incidentes

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

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

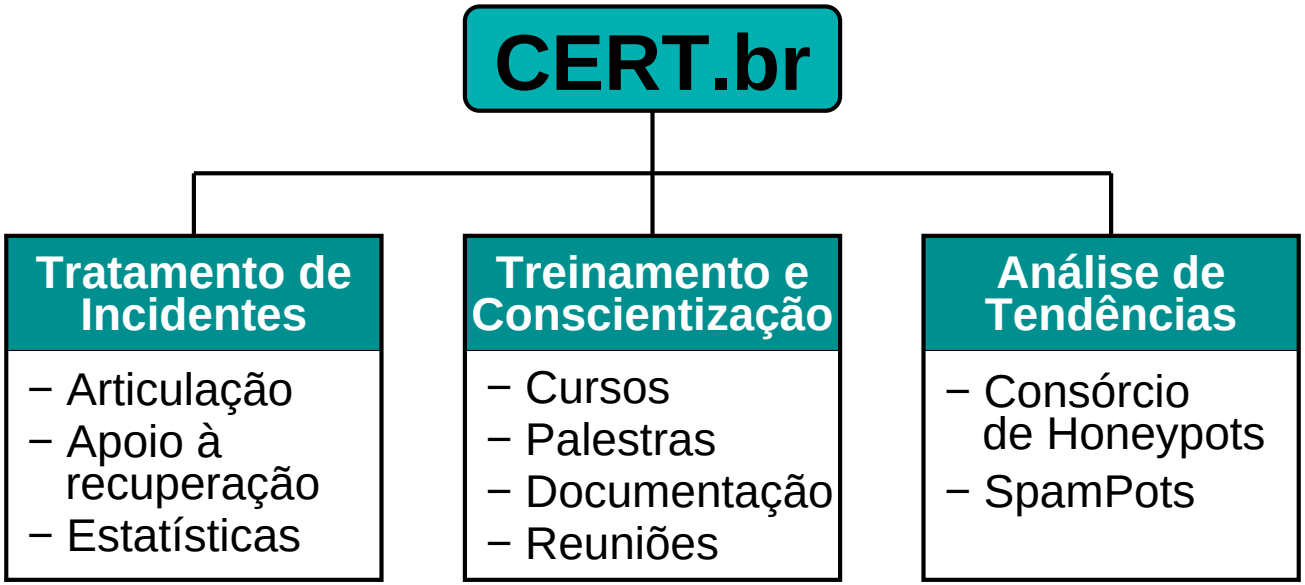
Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, 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**

Sobre o CERT.br

Criado em 1997 como ponto focal para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Agenda

Algumas Definições

Incidentes Mais Freqüentes e Recomedações para Prevenção e Tratamento

Acompanhamento de Notificações

Referências

Algumas Definições

Incidente de Segurança

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

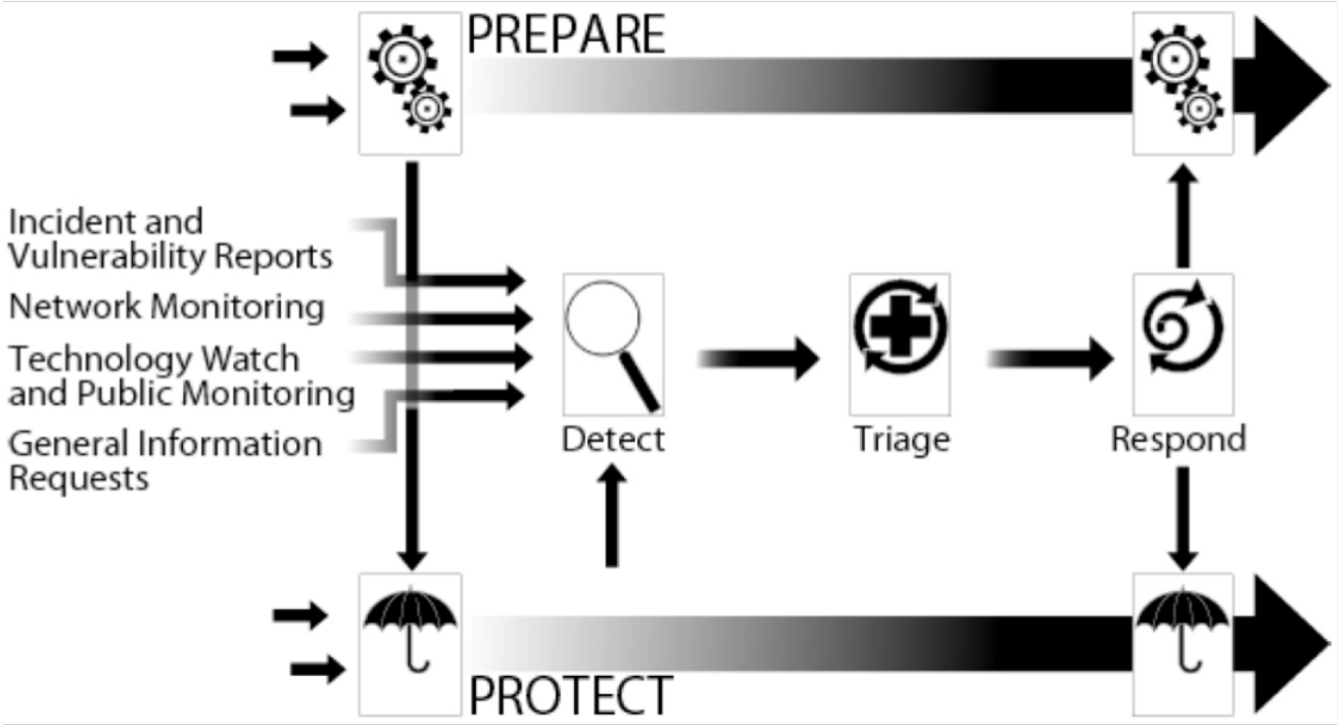
-ou-

O ato de violar uma política de segurança, explícita ou implícita.

http://www.cert.br/certcc/csirts/csirt_faq-br.html

CSIRT–*Computer Security Incident Response Team* e Tratamento de Incidentes

”Um CSIRT provê serviços de suporte para prevenção, tratamento e resposta a incidentes de segurança em computadores.”



Fonte: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Papel dos CSIRTs – Prevenção

- Definir políticas para tratamento de incidentes
- Auxiliar na proteção da infra-estrutura e das informações
- Conscientizar sobre os problemas
  - Administradores de redes e sistemas
  - Usuários
  - Administração superior

Papel dos CSIRTs – Resposta

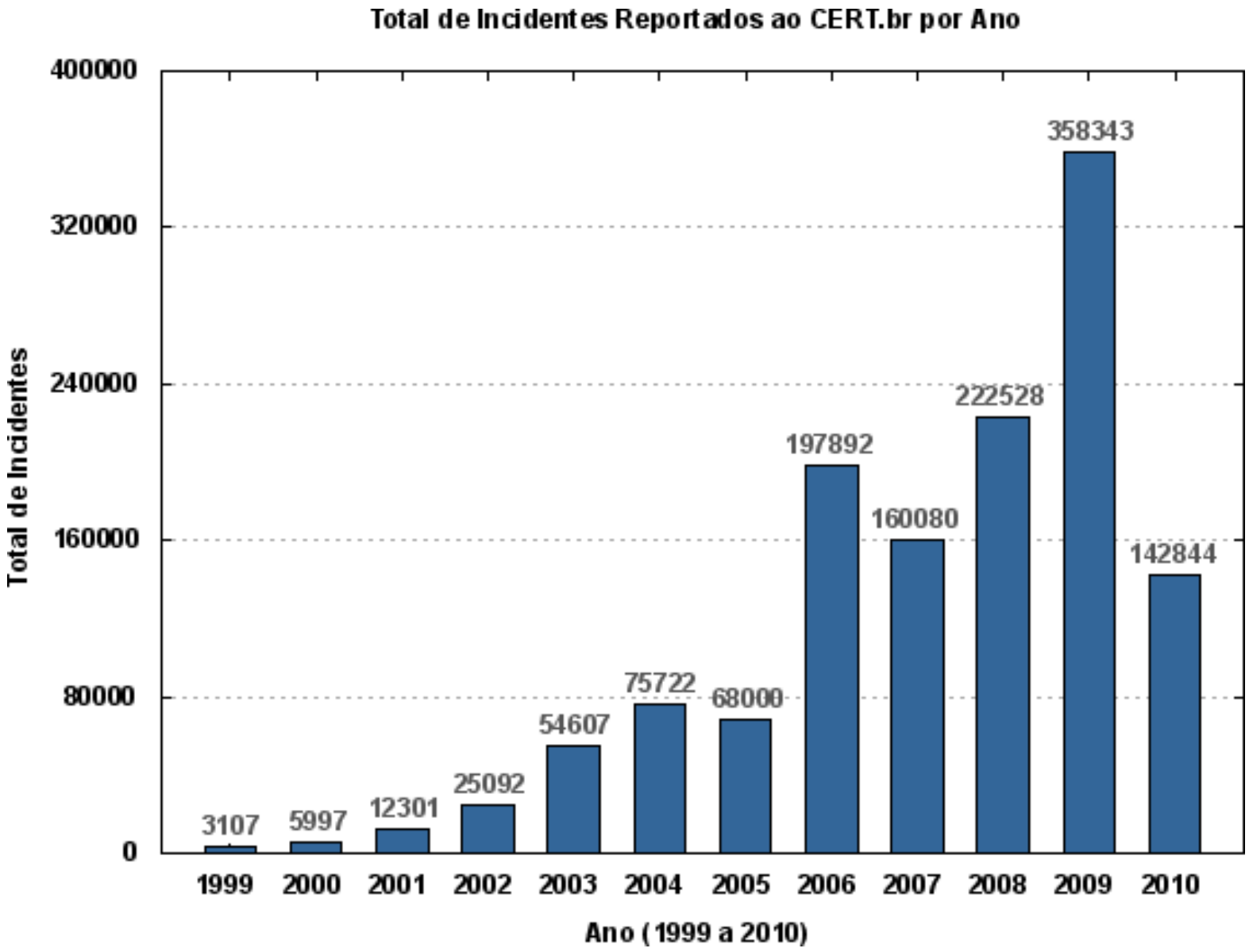
- Seguir as políticas
- Preservar as evidências em caso de possível ocorrência de um crime
- Responder o incidente – retornar o ambiente ao estado de produção
- A redução do impacto é conseqüência da:
  - agilidade de resposta
  - redução no número de vítimas
- O sucesso depende da confiabilidade
  - nunca divulgar dados sensíveis nem expor vítimas, por exemplo

Papel dos CSIRTs Quando se Fala em Crimes

- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime, por sempre lembrar de:
  - seguir as políticas
  - preservar as evidências
- O CSIRT não é um investigador
- A decisão de levar um caso à justiça deve ser da vítima
  - Em uma organização, leia-se: alta administração e setor jurídico

Incidentes Mais Freqüentes e Recomendações para Prevenção e Tratamento

Estatísticas do CERT.br – 1999–2010



Distribuição dos Incidentes Reportados ao CERT.br em 2010

Ataques mais Freqüentes – 2010

- de força bruta
  - SSH, FTP, Telnet, VNC, etc
- com contínuo crescimento nos últimos meses:
  - ataques a aplicações Web vulneráveis
  - servidores SIP
- a usuários finais
  - fraudes, *bots*, *spyware*, etc
  - motivação financeira
  - abuso de *proxies*, na maioria instalados por *bots*

Ataques de Força Bruta

Serviço SSH

- Ampla utilização em servidores UNIX
- Alvos
  - senhas fracas
  - contas temporárias
- Pouca monitoração permite que o ataque perdure por horas ou dias

Outros serviços

- FTP
- TELNET
- Radmin
- VNC

Mitigação de Força Bruta SSH

Recomendações:

- Senhas fortes
- Redução no número de equipamentos com serviço aberto para Internet
- Filtragem de origem
- Mover o serviço para uma porta não padrão
- Acesso somente via chaves públicas
- Aumento na monitoração

Detalhes em: http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Ataques a Servidores SIP

- Varreduras por dispositivos SIP
- Identificação de ramais válidos
- Tentativas de quebra de senhas de ramais
- Tentativas de realizar ligações
- spit?

Mitigação de Ataques SIP

Recomendações:

- Senhas fortes
- Redução no número de equipamentos com serviço aberto para Internet
- Filtragem de origem
- Aumento na monitoração
- Leituras recomendadas
  - Asterisk: `README-SERIOUSLY.bestpractices.txt`
  - *Seven Steps to Better SIP Security*: http://blogs.digium.com/2009/03/28/sip-security/
  - *Asterisk VoIP Security (webinar)*: http://www.asterisk.org/security/webinar/

Tentativas de Fraude Financeira

- *Spams* em nome de diversas entidades/temas variados
  - *links* para cavalos de tróia hospedados em diversos *sites*
  - vítima raramente associa o *spam* com a fraude financeira
- Páginas falsas estão voltando a ter números significativos
  - *drive-by downloads* sendo usados intensamente no Brasil – via JavaScript, ActiveX, etc, inclusive em grandes *sites*
  - em conjunto com *malware* modificando:
    - arquivo *hosts*
    - configuração de *proxy* em navegadores (arquivos PAC)
- *Malware* se registrando como *Browser Helper Objects* (BHO) em navegadores
- *Malware* validando, no *site* real, os dados capturados

Uso de *botnets* para DDoS

- 20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps
- Em março de 2009 foram atingidos picos de 48Gbps
  - em média ocorrem 3 ataques de 1Gpbs por dia na Internet
- De 2% a 3% do tráfego de um grande backbone é ruído de DDoS
- Extorsão é o principal objetivo
  - mas *download* de outros *malwares*, *spam* e furto de informações também valem dinheiro e acabam sendo parte do payload dos *bots*

Fonte: *Global Botnet Underground: DDoS and Botconomics*.
Jose Nazario, Ph.D., Head of Arbor ASERT
Keynote do Evento RioInfo 2009.

Brasil na CBL

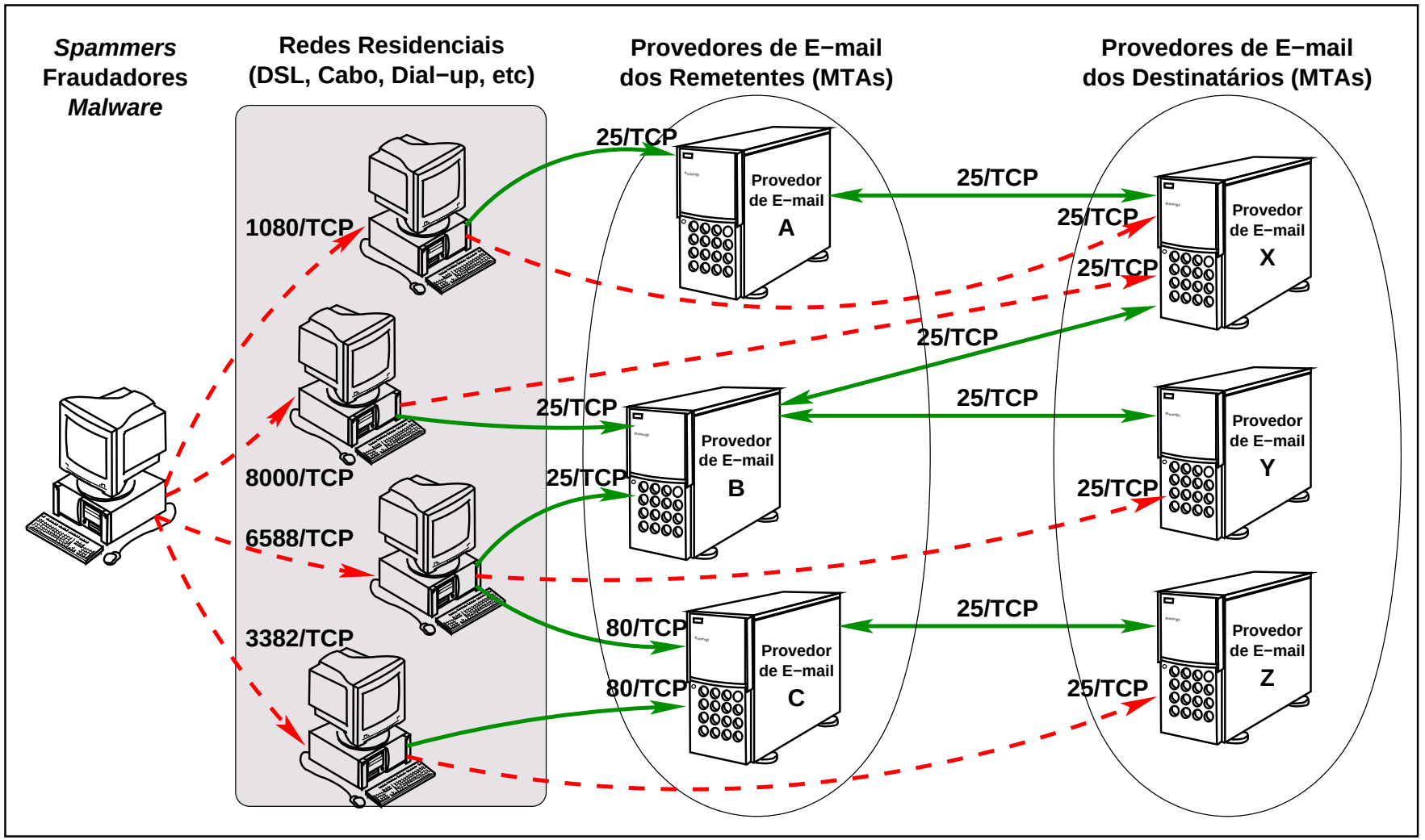
	País	Endereços IP	% do Total	Taxa de Infecção (%)
1	Índia (IN)	1.129.747	17,06	4,881
2	Brasil (BR)	630.446	9,52	1,234
3	Rússia (RU)	585.637	8,84	1,672
4	Vietnã (VN)	319.472	4,82	2,840
5	Ucrânia (UA)	313.528	4,73	3,415
6	Indonésia (ID)	213.132	3,22	2,390
7	China (CN)	198.271	2,99	0,071
8	Tailândia (TH)	171.941	2,60	1,712
9	Paquistão (PK)	164.467	2,48	4,667
10	Itália (IT)	154.803	2,34	0,355

Fonte: CBL, uma lista de endereços IP de computadores que comprovadamente enviaram *spams* nas últimas 24 horas e estavam infectados.

Dados gerados em: `Mon Jan 17 11:37:41 2011 UTC/GMT`

`Composite Blocking List` http://cbl.abuseat.org/

Abuso de Máquinas Infectadas para Envio de Spam



Mitigação do Abuso das Máquinas de Usuários

- definição de políticas de uso aceitável;
- monitoração proativa de fluxos;
- monitoração das notificações de abusos;
- ação efetiva junto ao usuário nos casos de detecção de *proxy* aberto ou máquina comprometida;
- *egress filtering*;
- gerência de saída de tráfego com destino à porta 25/TCP.

Prevenção de DNS *Cache Poisoning*

- Instalar as últimas versões dos *softwares* DNS
  - Correções usam portas de origem aleatórias nas consultas
  - Não eliminam o ataque, apenas retardam seu sucesso

- Adoção de DNSSEC é uma solução mais definitiva

http://registro.br/suporte/tutoriais/dnssec.html

Acompanhamento de Notificações

- Criar *e-mails* da RFC 2142 (`security@`, `abuse@`)
- Manter os contatos de Whois atualizados
- O contato técnico deve ser um profissional que tenha contato com as equipes de abuso
  - ou, ao menos, saber para onde redirecionar notificações e reclamações
- Redes com grupos de resposta a incidentes de segurança devem anunciar o endereço do grupo junto à comunidade
- As contas que recebem notificações de incidentes ou abusos não podem barrar mensagens
  - antivírus podem impedir uma notificação de *malware*
  - regras anti-spam podem impedir notificações de *spam* e de *phishing*

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/