Boas Práticas de Segurança

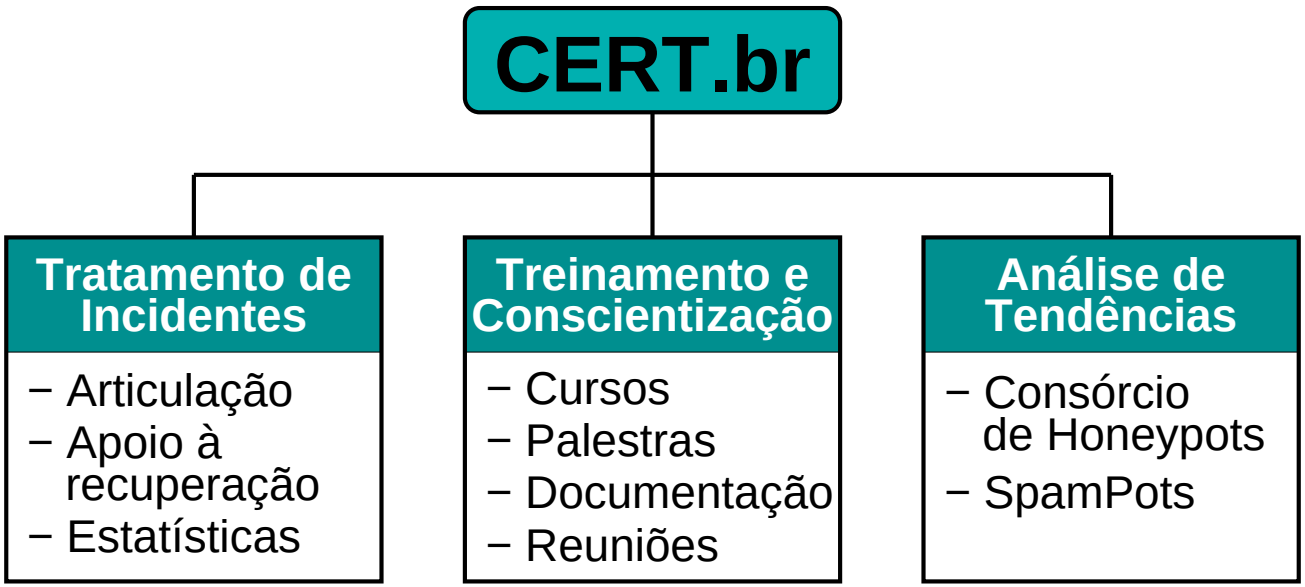
Klaus Steding-Jessen
jessen@cert.br
Cristine Hoepers
cristine@cert.br

Esta Apresentação:
http://www.cert.br/docs/palestras/

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

Sobre o CERT.br

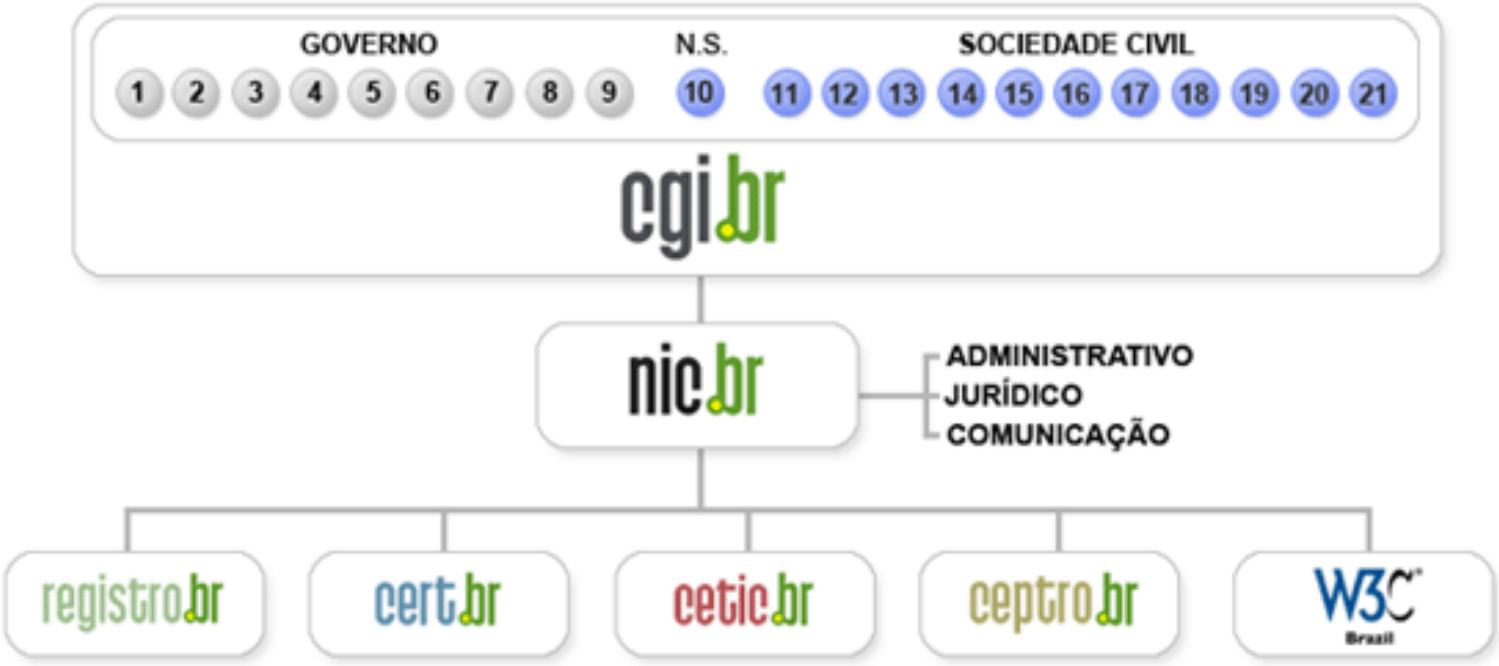
Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER
APWG
SEIPartner CERT Courses
The Honeynet PROJECT®

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

Estrutura do CGI.br



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

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**

Motivação

Objetivos da implementação de boas práticas

- Reduzir o desperdício de recursos
- Não ser origem de ataques
- Prover um serviço de maior qualidade
- Colaborar para o aumento da segurança da Internet

Não será possível erradicar todos os problemas, precisamos torná-los gerenciáveis

- cada setor precisa fazer a sua parte – cooperação para a solução dos problemas
- a solução não virá de uma ação única

Agenda

Ataques mais Freqüentes
    Prevenção e Mitigação

Estruturação e Atuação das Áreas de Segurança

Considerações Finais

Referências

Ataques mais Freqüentes e Recomendações para Prevenção e Mitigação

Ataques mais Freqüentes

Reportados ao CERT.br no terceiro trimestre de 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:

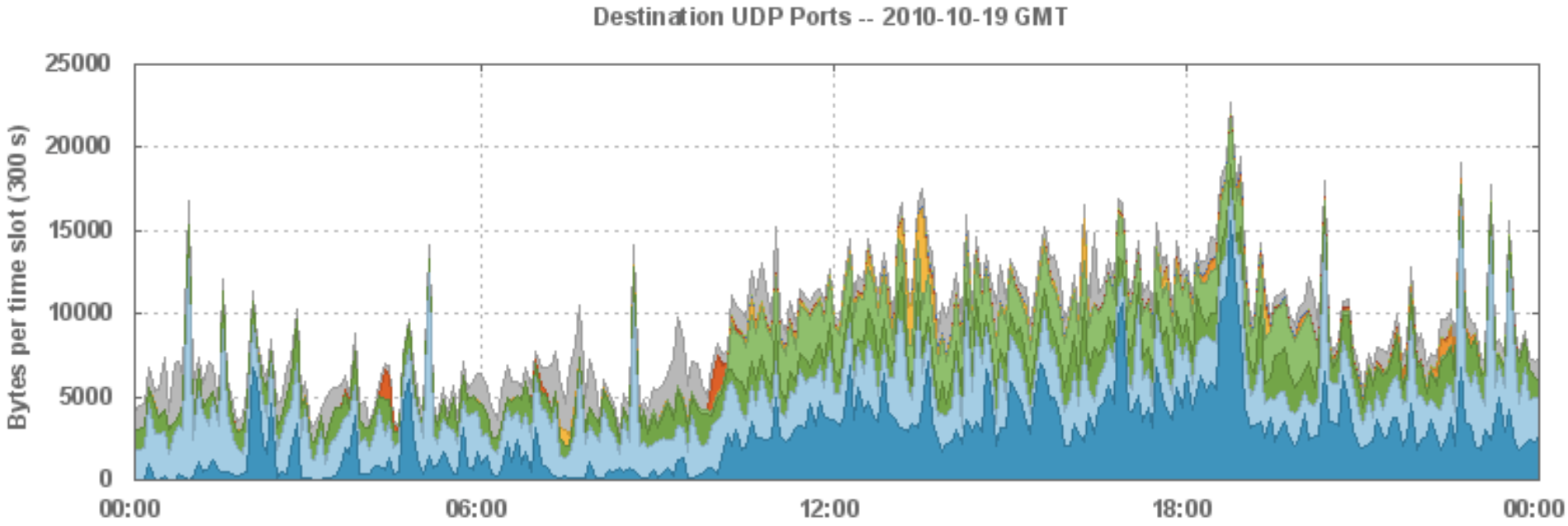
- Senhas fortes
- Redução no número de equipamentos com serviço aberto para Internet
- Filtragem de origem
- Mover o serviço para uma porta não padrão
- Acesso somente via chaves públicas
- Aumento na monitoração

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?

Varreduras SIP no Consórcio de Honeypots



#	Key	Port	Name	Total		Max
01		137	NETBIOS Name Service	765.56 kB	28.75 %	51.88 B/s
02		5060	SIP (Session Initiation Protocol)	762.02 kB	28.62 %	44.20 B/s
03		1434	Microsoft SQL Monitor	406.32 kB	15.26 %	11.11 B/s
04		161	SNMP (Simple Network Management Protocol)	319.79 kB	12.01 %	11.23 B/s
05		53	DNS (Domain Name System)	42.80 kB	1.61 %	20.16 B/s

SIP: OPTIONS

```
U 2010/09/28 22:54:07.491696 89.47.63.183:59317 -> network_server:5060
  OPTIONS sip:100@network_server SIP/2.0..Via: SIP/2.0/UDP 127.0.1.1:5060;bra
  nch=z9hG4bK-3932320937;rport..Content-Length: 0..From: "sipvicious"<sip:100
  @1.1.1.1>; tag=6338616232316238313363340132333530383633323634..Accept: appl
  ication/sdp..User-Agent: friendly-scanner..To: "sipvicious"<sip:100@1.1.1.1
  >..Contact: sip:100@127.0.1.1:5060..CSeq: 1 OPTIONS..Call-ID: 3655079754140
  81403837664..Max-Forwards: 70....

U 2010/09/28 22:54:07.580669 network_server:5060 -> 89.47.63.183:59317
  SIP/2.0 200 OK..Call-id: 365507975414081403837664..Cseq: 1 OPTIONS..From: "
  sipvicious"<sip:100@1.1.1.1>; tag=6338616232316238313363340132333530383633323
  23634..To: "sipvicious"<sip:100@1.1.1.1>..Via: SIP/2.0/UDP 127.0.1.1:5060;b
  ranch=z9hG4bK-3932320937;received=89.47.63.183;rport=59317..Server: Asteris
  k PBX 1.2.22..Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, N
  OTIFY, INFO..Supported: replaces, timer..Contact: <sip:network_server>..Acc
  ept: application/sdp..Content-length: 0....
```

SIP: REGISTER

```
2010-10-20 05:57:55 IP: 211.103.141.180, method: REGISTER,
from: "123", to: "123", CSeq: "1 REGISTER", user-agent: "friendly-scanner"

[...] from: "1234", to: "1234", [...]
[...] from: "12345", to: "12345", [...]
[...] from: "123456", to: "123456", [...]
[...] from: "sip", to: "sip", [...]
[...] from: "admin", to: "admin", [...]
[...] from: "pass", to: "pass", [...]
[...] from: "password", to: "password", [...]
[...] from: "testing", to: "testing", [...]
[...] from: "guest", to: "guest", [...]
[...] from: "voip", to: "voip", [...]
[...] from: "account", to: "account", [...]
[...] from: "passwd", to: "passwd", [...]
[...] from: "qwerty", to: "qwerty", [...]
[...] from: "654321", to: "654321", [...]
[...] from: "54321", to: "54321", [...]
[...] from: "4321", to: "4321", [...]
[...] from: "abc123", to: "abc123", [...]
[...] from: "123abc", to: "123abc", [...]
```

SIP: INVITE

```
U 2010/09/30 23:50:21.236653 67.21.82.4:45018 -> network_server:5060
  INVITE sip:96626653000@network_server SIP/2.0..Via: SIP/2.0/UDP 67.21.82.4:
  45018;rport;branch=z9hG4bK051C0283E05B4BF182275668E1F3BD15..From: 102 <sip:
  102@network_server>;tag=129156506..To: <sip:96626653000@network_server>..Co
  ntact: <sip:102@67.21.82.4:45018>..Call-ID: 3A1309F9-9FAC-4BE3-8B7E-9294496
  D1E08@192.168.1.3..CSeq: 9999 INVITE..Max-Forwards: 70..Content-Type: appli
  cation/sdp..User-Agent: X-PRO build 1101..Content-Length: 312....v=0..o=102
   4272671 4272671 IN IP4 67.21.82.4..s=X-PRO..c=IN IP4 67.21.82.4..t=0 0..m=
  audio 45020 RTP/AVP 0 8 3 18 98 97 101..a=rtpmap:0 pcmu/8000..a=rtpmap:8 pc
  ma/8000..a=rtpmap:3 gsm/8000..a=rtpmap:18 G729/8000..a=rtpmap:98 iLBC/8000.
  .a=rtpmap:97 speex/8000..a=rtpmap:101 telephone-event/8000..a=fmtp:101 0-15
  ..
```

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.

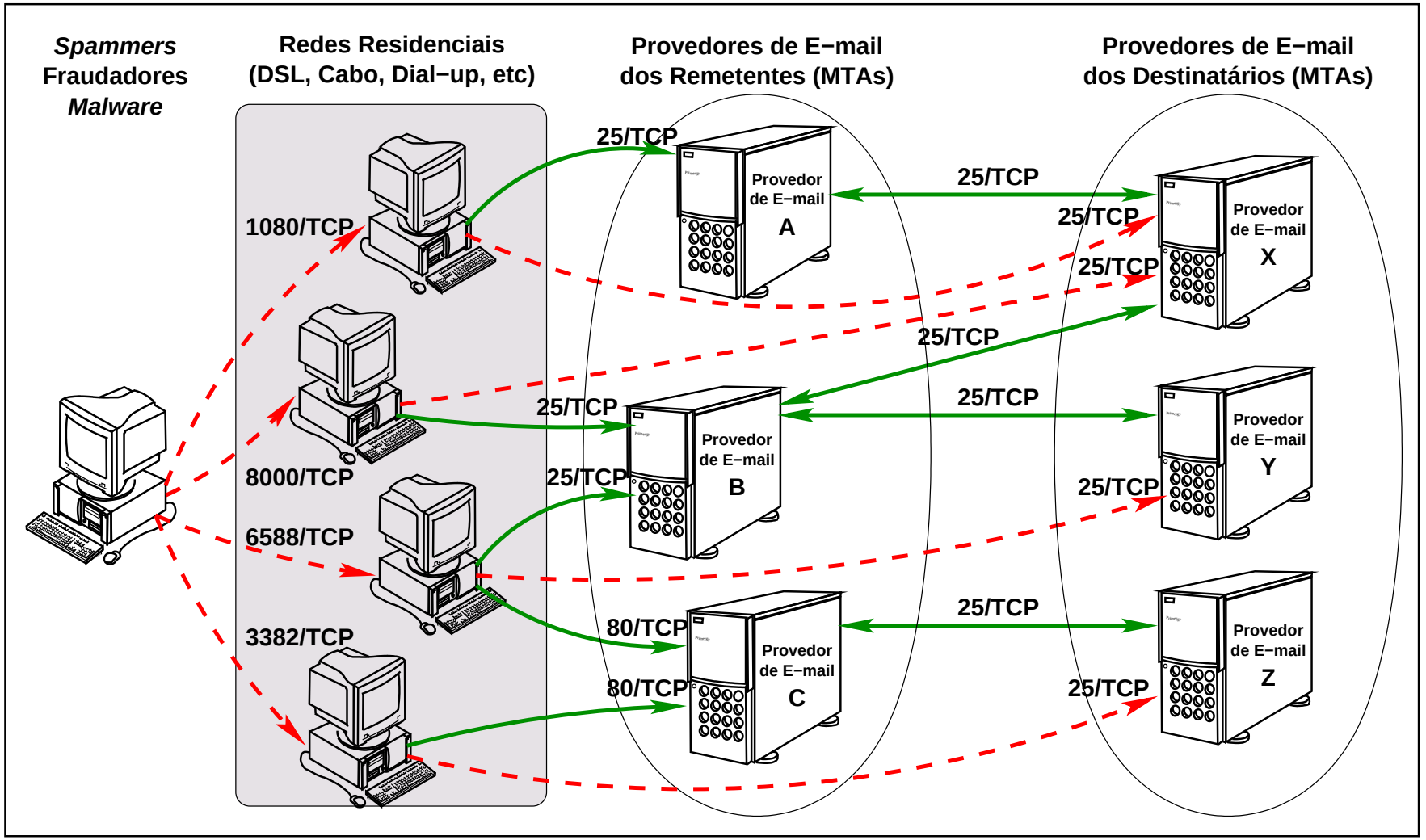
Brasil na CBL

	País	Endereços IP	% do Total	Taxa de Infecção (%)
1	Índia (IN)	1.317.675	16,93	6,495
2	Brasil (BR)	765.770	9,84	1,560
3	Rússia (RU)	627.210	8,06	1,920
4	Vietnã (VN)	504.292	6,48	4,543
5	Ucrânia (UA)	310.113	3,98	3,858
6	Indonésia (ID)	252.074	3,24	2,786
7	Paquistão (PK)	203.876	2,62	5,939
8	Tailândia (TH)	202.541	2,60	2,365
9	Arábia Saudita (SA)	171.831	2,21	4,793
10	EUA (US)	163.046	2,09	0,013

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

Dados gerados em: `Thu Oct 7 16:42:47 2010 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.

Gerência de Porta 25

Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

Implementação depende da aplicação de medidas por provedores e operadoras:

- Provedores de serviços de correio eletrônico:
  - Implementar o padrão de *Message Submission*, tipicamente na porta 587/TCP (RFC 4409), e implementar SMTP autenticado
- Operadoras de banda larga/*dial up* de perfil residencial (usuário final):
  - Impedir envio direto de mensagens eletrônicas (através da filtragem da saída de tráfego com destino à porta 25/TCP)

Detalhes em: http://www.antispam.br/admin/porta25/

Benefícios da Gerência de Porta 25

- Saída dos blocos do ASN de listas de bloqueio
- Diminuição de reclamações de usuários
- Dificulta o abuso da infra-estrutura da Internet para atividades ilícitas (fraudes, furto de dados, etc)
- Aumento de rastreabilidade em caso de abuso
- Atua na submissão, antes da mensagem entrar na infra-estrutura de *e-mail*
- Diminuição do consumo de banda por *spammers*
- Diminuição de custos operacionais
  - spam foi o mais apontado como responsável pela demanda de recursos operacionais no "*2008 Worldwide Infrastructure Security Report*"

    http://www.arbornetworks.com/report

Outras Recomendações

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

Correção de DNS Recursivo Aberto

Duas possíveis soluções:

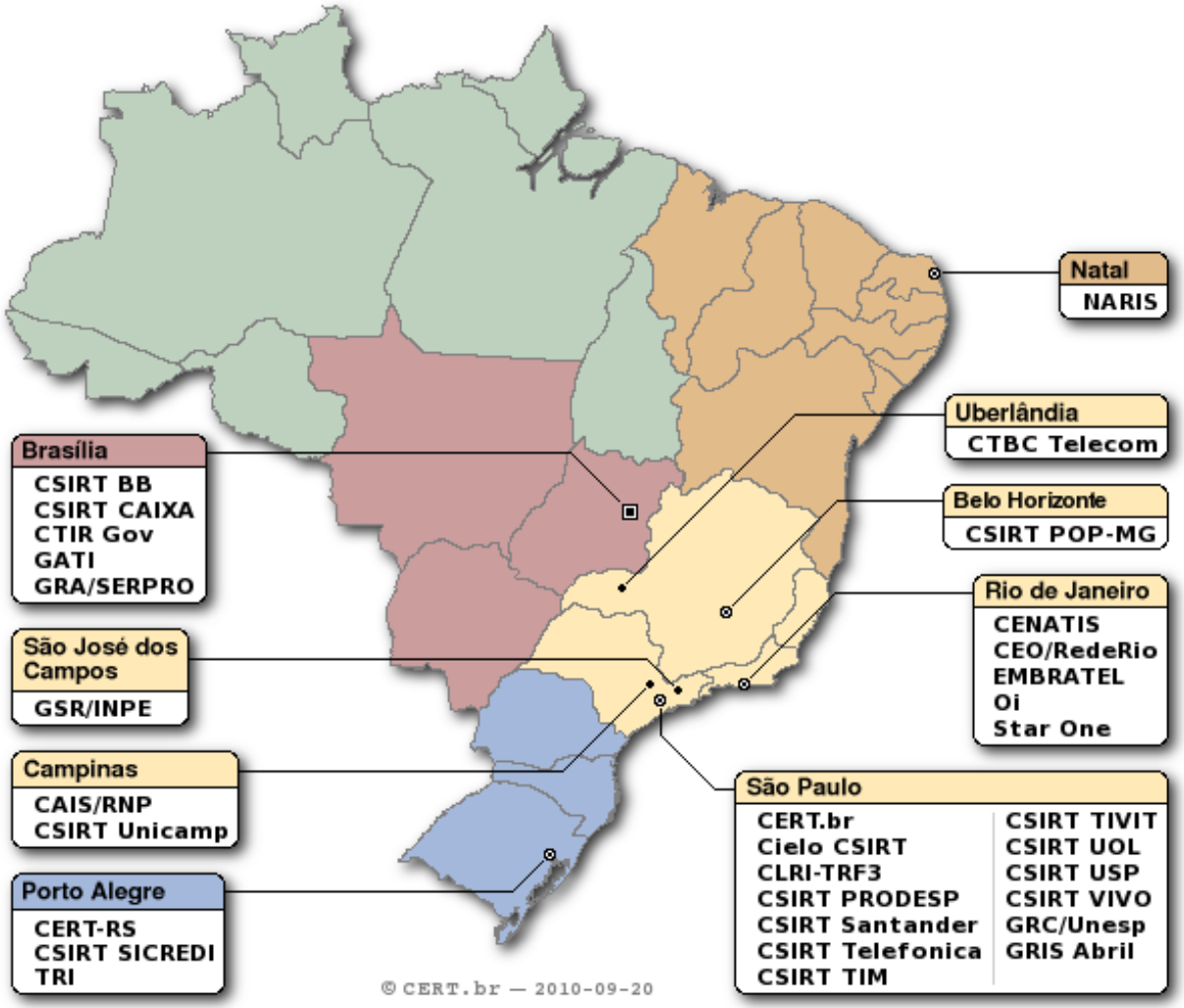
- Colocar os servidores DNS em computadores diferentes, com configurações e políticas de acesso diferentes; ou
  - única solução possível para o Microsoft DNS
- Utilizar o conceito de *views* do BIND

Detalhes em: http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

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*

Criar um Grupo de Tratamento de Incidentes



http://www.cert.br/csirts/brasil/

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

Papel dos CSIRTs

- A redução do impacto de um incidente 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
- O papel do CSIRT e dos profissionais de segurança é:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
  - responder incidentes – retornar o ambiente ao estado de produção
- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências

Considerações Finais

Considerações Finais

- Monitore o tráfego de saída de sua rede
- Tenha um ponto de contato para assuntos de segurança e abuso
  - atue e dê algum tipo de resposta a quem entrou em contato
- Mantenha-se informado
  - listas dos fabricantes de *software*
  - *sites*, blogs e listas de segurança
- Cada um é responsável por uma parte da segurança da Internet

Referências

- Esta Apresentação:
  http://www.cert.br/docs/palestras/
- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/