Estado da Segurança na Internet e Tecnologias para Prevenção e Monitoração de Eventos

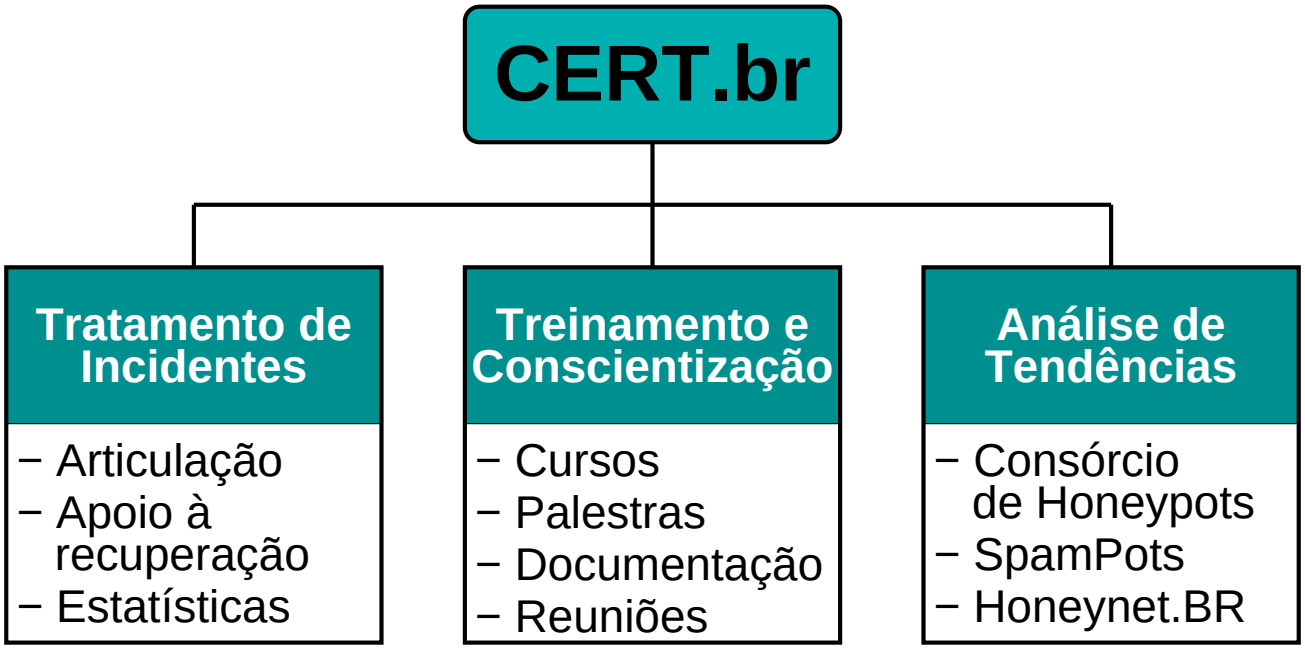
Cristine Hoepers
cristine@cert.br
Klaus Steding-Jessen
jessen@cert.br

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

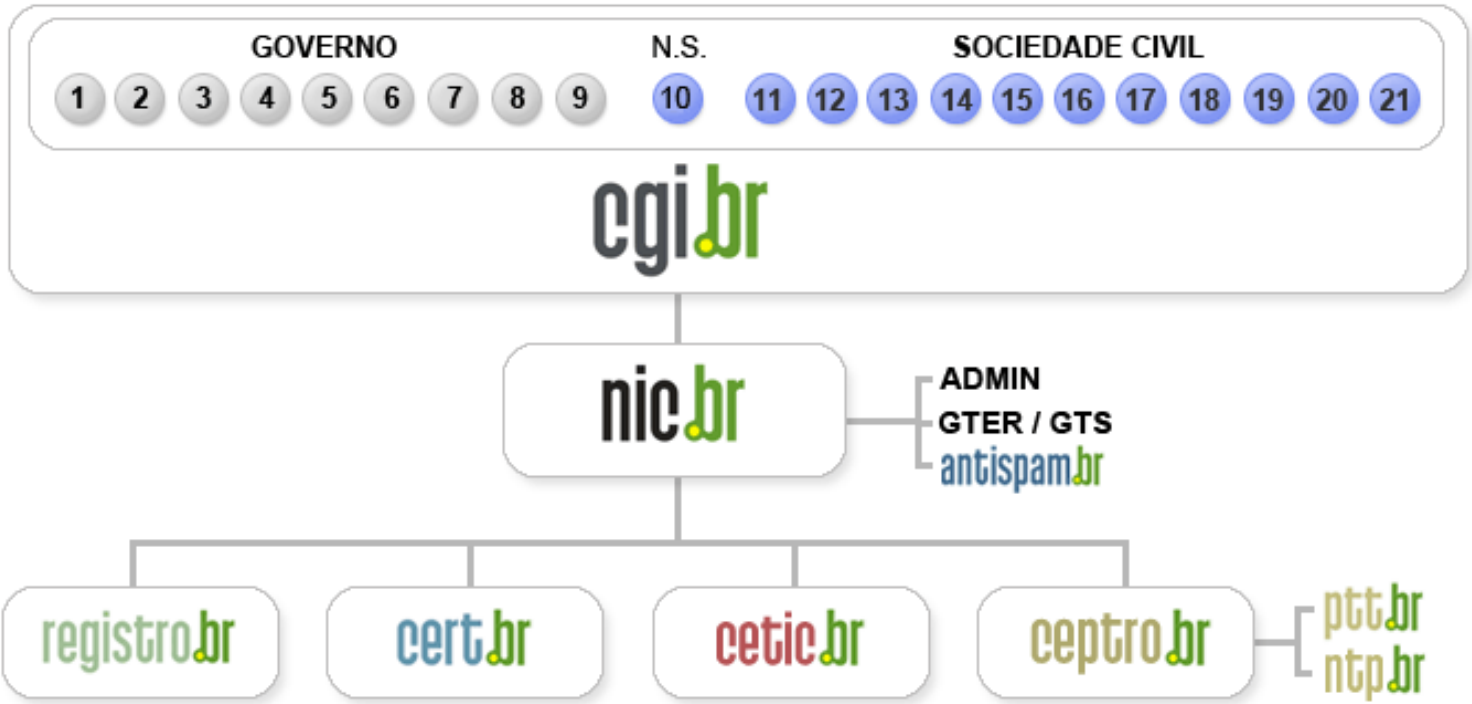
APWG

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**

Agenda

- A evolução da Internet e dos problemas de segurança
- Qual a situação atual
  - dados sobre segurança e incidentes na Internet
  - ameaças atuais
- Prevenção
- Tecnologias de monitoração
- Estudos de casos de uso de *honeypots* e *flows* para monitoração de redes

Evolução dos Problemas de Segurança

Final dos Anos 60

Início da Internet

- Projeto não considera implicações de segurança
- Comunidade de pesquisadores
- Novas instituições eram conectadas com base em uma relação de confiança

"*Where Wizards Stay Up Late: The Origins Of The Internet*", Katie Hafner & Matthew Lyon
(ISBN-13: 978-0684832678)

Anos 80

Invasores com

- Alto conhecimento
- Dedicação por longos períodos para realização de poucos ataques

"*Cukoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*", Cliff Stoll
(ISBN-13: 978-0671726881)

- 30+ sistemas invadidos
- Contas/senhas fracas
- Vulnerabilidades em *softwares*
- Tempo e persistência

Final dos Anos 80

- Primeiro *worm* com maiores implicações de segurança
  - Criado por Robert Morris Jr.
  - Explorava a combinação de vulnerabilidades no sendmail, fingerd e em configurações dos *"r" services*
  - Mais de 6000 computadores atingidos
- Aproximadamente 10% da Internet na época
- Mobilização em torno do tema segurança
- Criação do CERT/CC 15 dias após

ftp://coast.cs.purdue.edu/pub/doc/morris_worm/
http://www.cert.org/archive/pdf/03tr001.pdf
http://www.ietf.org/rfc/rfc1135.txt

Anos 1991–2001

- Início da utilização da “engenharia social” em grande escala
- Primeiros ataques remotos a sistemas
- Popularização de: cavalos de tróia, furto de senhas, varreduras em busca de máquinas vulneráveis, captura de informações (*sniffers*), ataques de negação de serviço, etc
- Primeiras ferramentas automatizadas para
  - Realizar invasões
  - Ocultar a presença dos invasores (*rootkits*)
- Sofisticação no processo de controle das ferramentas

Anos 2002–2005

- Explosão no número de códigos maliciosos com diversos fins
  - *worms*, *bots*, cavalos de tróia, vírus, *spyware*
- Códigos com múltiplas funcionalidades
  - Múltiplos vetores de ataque, código eficiente, aberto e facilmente adaptável
- Permitem controle remoto
- Praticamente não exigem interações por parte dos invasores

Situação Atual

Características dos Ataques

- Crime organizado
  - Aliciando *spammers* e invasores
  - Injetando dinheiro na "economia *underground*"
- *Botnets*
  - Usadas para envio de *scams*, *phishing*, invasões, esquemas de extorsão
- Redes mal configuradas sendo abusadas para realização de todas estas atividades
  - sem o conhecimento dos donos
- Amplo uso de ferramentas automatizadas de ataque
- **Alvo migrou para usuários finais**

Características dos Atacantes

- Em sua maioria pessoal com pouco conhecimento técnico que utiliza ferramentas prontas
- Trocam informações no *underground*
- Usam como moedas de troca
  - Senhas de administrador/`root`
  - Novos *exploits*
  - Contas/senhas de banco
  - Números de cartão de crédito
  - *bots*/*botnets*
- Atacantes + *spammers*

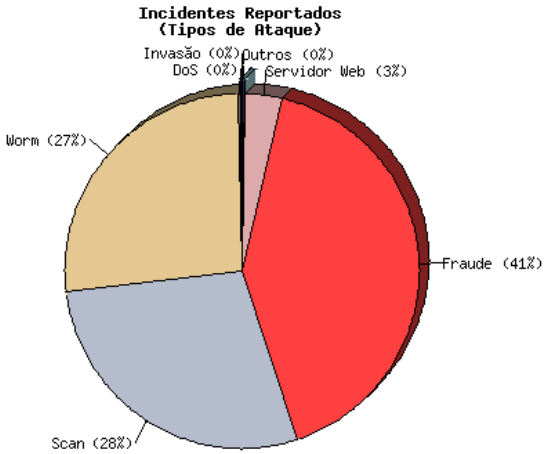
Principais Vulnerabilidades

- Pouco enfoque em Segurança de *Software* e Programação Segura
  - vulnerabilidades freqüentes
- Sistemas operacionais e *softwares* desatualizados
- Códigos maliciosos explorando essas vulnerabilidades em curto espaço de tempo

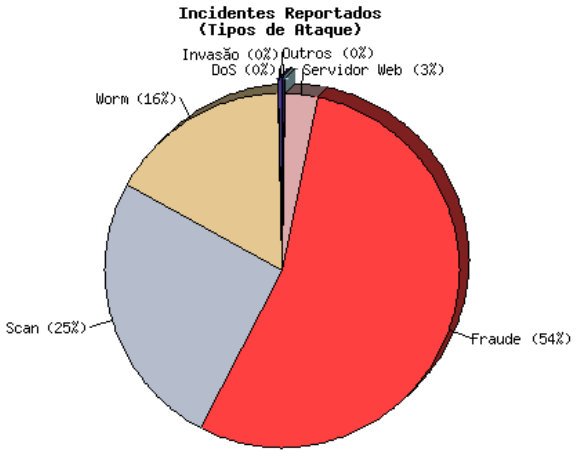
Problemas mais Freqüentes

Tentativas de Fraude

2008 — Jan–Mar



2007 — Abr–Jun



Totais da categoria fraude:

2004	4.015	(05%)
2005	27.292	(40%)
2006	41.776	(21%)
2007	45.298	(28%)
2008	36.561	[Jan–Jun]

Características das tentativas de fraude:

- **Em nome de várias instituições, com tópicos diversos**
- **Com links para cavalos de tróia**

Fonte:
http://www.cert.br/stats/incidentes/

Histórico das Fraudes no Brasil

2001 *Keyloggers* enviados por *e-mail*, ataques de força bruta

2002–2003 Casos de *phishing* e uso disseminado de servidores DNS comprometidos

2003–2004 Aumento dos casos de *phishing* mais sofisticados

- Dados eram enviados dos *sites* falsificados para *sites* coletores
- *Sites* coletores processavam os dados e os enviavam para contas de *e-mail*

2005–2006 *Spams* usando nomes de diversas entidades e temas variados

- *Links* para cavalos de tróia hospedados em diversos *sites*
- Vítima raramente associa o *spam* recebido com a fraude financeira

2007–hoje *downloads* involuntários, via códigos JavaScript, ActiveX, etc, em máquinas vulneráveis

- continuidade das tendências de 2005–2006

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

- Radmin
- VNC

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

Vulnerabilidades no DNS

Cache Poisoning

- Permite redirecionamento de domínios para IPs com conteúdo malicioso
- Facilitado pelo ataque descoberto por Dan Kaminsky

http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Servidores recursivos abertos

- Permitem que qualquer máquina faça consultas
- Podem ser usados como amplificadores em ataques de DDoS

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

Prevenção

Quem Participa da Prevenção

- Desenvolvedores
- Administradores de Redes e Profissionais de Segurança
- Usuários

Desenvolvedores

Segurança de *Software*

- Levantar requisitos de segurança em todo o ciclo de vida do *software*
- Aplicar práticas de programação segura
- Sites de referência:
  - http://www.securecoding.org/
  - http://www.securecoding.cert.org/
  - http://www.cert.org/secure-coding/
  - http://buildsecurityin.us-cert.gov/

Série de Livros da *Addison-Wesley*

http://www.buildsecurityin.com/

Administradores de Redes e Profissionais de Segurança

Proteger a Infra-Estrutura

Instalar a última versão e aplicar as correções de segurança (*patches*)

- Sistemas operacionais
- Serviços de rede, como DNS, Web, SMTP, etc
- Aplicativos
  - navegador, processador de textos, leitor de *e-mails*, visualizador de imagens, PDFs e vídeos, etc
- *Hardware*
  - *firmware* de *switches*, equipamentos *wireless*, etc

Medidas Adicionais

- Definir Políticas e Procedimentos
- Implementar práticas de segurança em camadas
  - *firewalls*, IDSs, antivírus, autenticação, criptografia, etc
- Conhecer e monitorar o tráfego de sua rede
- Manter-se atualizado
  - treinamentos
  - conferências
  - listas de discussão
  - *sites* e *blogs* de segurança

Usuários Finais

Utilizar Programas de Segurança

- aplicar as atualizações do sistema e dos aplicativos
- *firewall* pessoal
- antivírus
  - atualizar as assinaturas diariamente
- anti-*spyware*
- anti-*spam*
- extensões em navegadores
  - gerência de JavaScript, *cookies*, etc

Melhorar a Postura On-line (1/3)

- Não acessar *sites* ou seguir *links*
  - recebidos por *e-mail*
  - recebidos por serviços de mensagem instantânea
  - presentes em páginas sobre as quais não se saiba a procedência
- Receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade
  - códigos maliciosos se propagam a partir das contas de máquinas infectadas
  - fraudadores se fazem passar por instituições confiáveis

Melhorar a Postura On-line (2/3)

Precauções com contas e senhas

- utilizar uma senha diferente para cada serviço/*site*
- evitar senhas fáceis de adivinhar
  - nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários
- usar uma senha composta de letras, números e símbolos
- utilizar o usuário Administrador ou `root` somente quando for estritamente necessário
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Melhorar a Postura On-line (3/3)

Não fornecer em páginas *Web*, *blogs* e *sites* de redes de relacionamentos:

- seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc)
- dados sobre o seu computador ou sobre os *softwares* que utiliza
- informações sobre o seu cotidiano
- informações sensíveis, como senhas e números de cartão de crédito

Informar-se e Manter-se Atualizado

- http://cartilha.cert.br/
- http://www.antispam.br/

Tecnologias de Monitoração

Mudança de Perspectiva

- Redes cada vez mais velozes
- Ataques utilizam criptografia
- Necessário ter uma visão global
- Tecnologias usadas
  - análise de fluxos de rede (*flows*)
  - *honeypots*

Análise de *Flows*

- Permite monitorar um grande volume de dados
- Foco em identificar anomalias no tráfego
  - picos de tráfego
  - protocolos e serviços incomuns
- Ferramentas de código aberto disponíveis
  - https://www.cert.org/netsa/
  - http://www.caida.org/tools/
  - http://qosient.com/argus/

Honeypots de Baixa Interatividade

- Emulam serviços e sistemas
- O atacante não tem acesso ao sistema operacional real
- O atacante não compromete o *honeypot*
- Fácil de configurar e manter
- Baixo risco
- Informações obtidas são limitadas
- Exemplos:
  - Honeyd – http://www.honeyd.org/
  - Nepenthes – http://nepenthes.mwcollect.org/
- Livro: "*Virtual Honeypots: From Botnet Tracking to Intrusion Detection*"

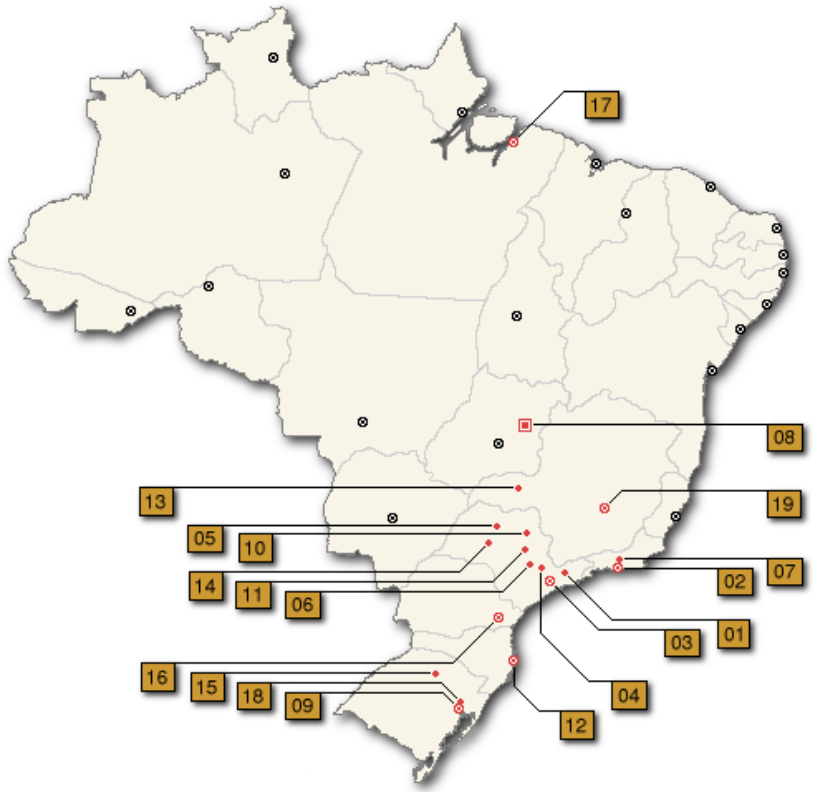
  http://www.informit.com/store/product.aspx?isbn=0321336321

Estudos de Casos de Uso de *Honeypots* e *Flows* para Monitoração de Redes

Consórcio Brasileiro de *Honeypots*

Múltiplos *honeypots* de baixa interatividade no espaço Internet brasileiro, com o objetivo de:

- aumentar a capacidade de:
  - detecção de incidentes
  - correlação de eventos
  - determinação de tendências de ataques
- atuar em conjunto com CSIRTs para a difusão das informações



http://www.honeypots-alliance.org.br/

Instituições Consorciadas

- 37 instituições consorciadas
  - indústria, provedores de telecomunicações, redes acadêmicas, governamentais e militares
- Seguem as políticas e procedimentos do projeto
- Cada instituicao fornece:
  - equipamento e rede
  - manutenção do(s) *honeypot*(s)
- A coordenação do projeto precisa conhecer e aprovar as instituições antes de serem consorciadas

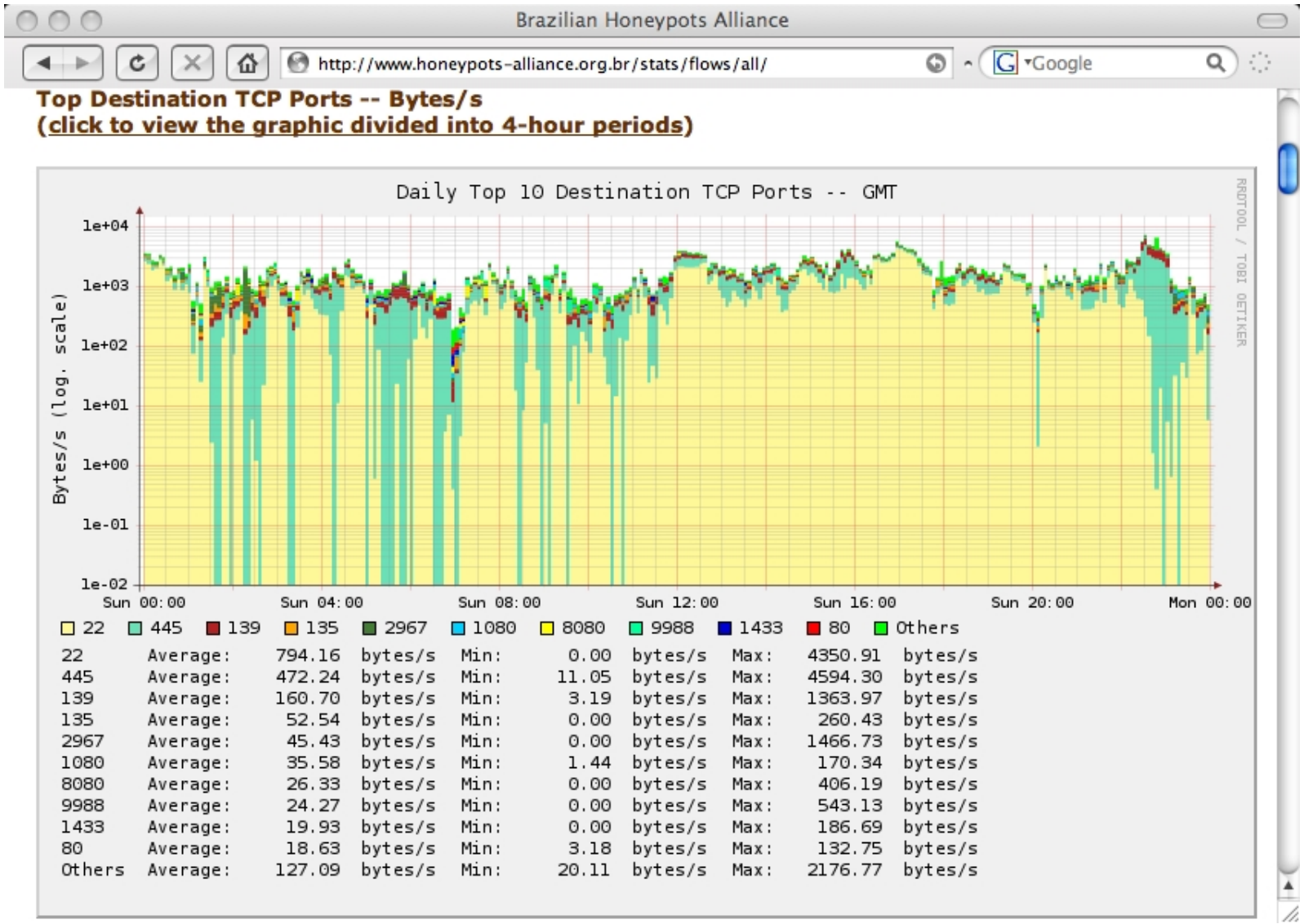
Configuração dos *Honeypots*

- Honeyd - http://www.honeyd.org/
  - Emula diferentes SOs
  - Executa *listeners* para emular serviços (IIS, `ssh`, `sendmail`, etc)
- Arpd - http://www.honeyd.org/tools.php
  - *proxy arp* usando um bloco de endereçamento de rede (de /28 a /21)
  - 1 IP para gerenciamento do *honeypot*
  - Outros IPs usados na emulação de diversos SOs e serviços
- OpenBSD pf - http://www.openbsd.org/faq/pf/
  - *Logs* completos do tráfego de rede
  - Formato `libpcap`

Servidor de Coleta dos Dados

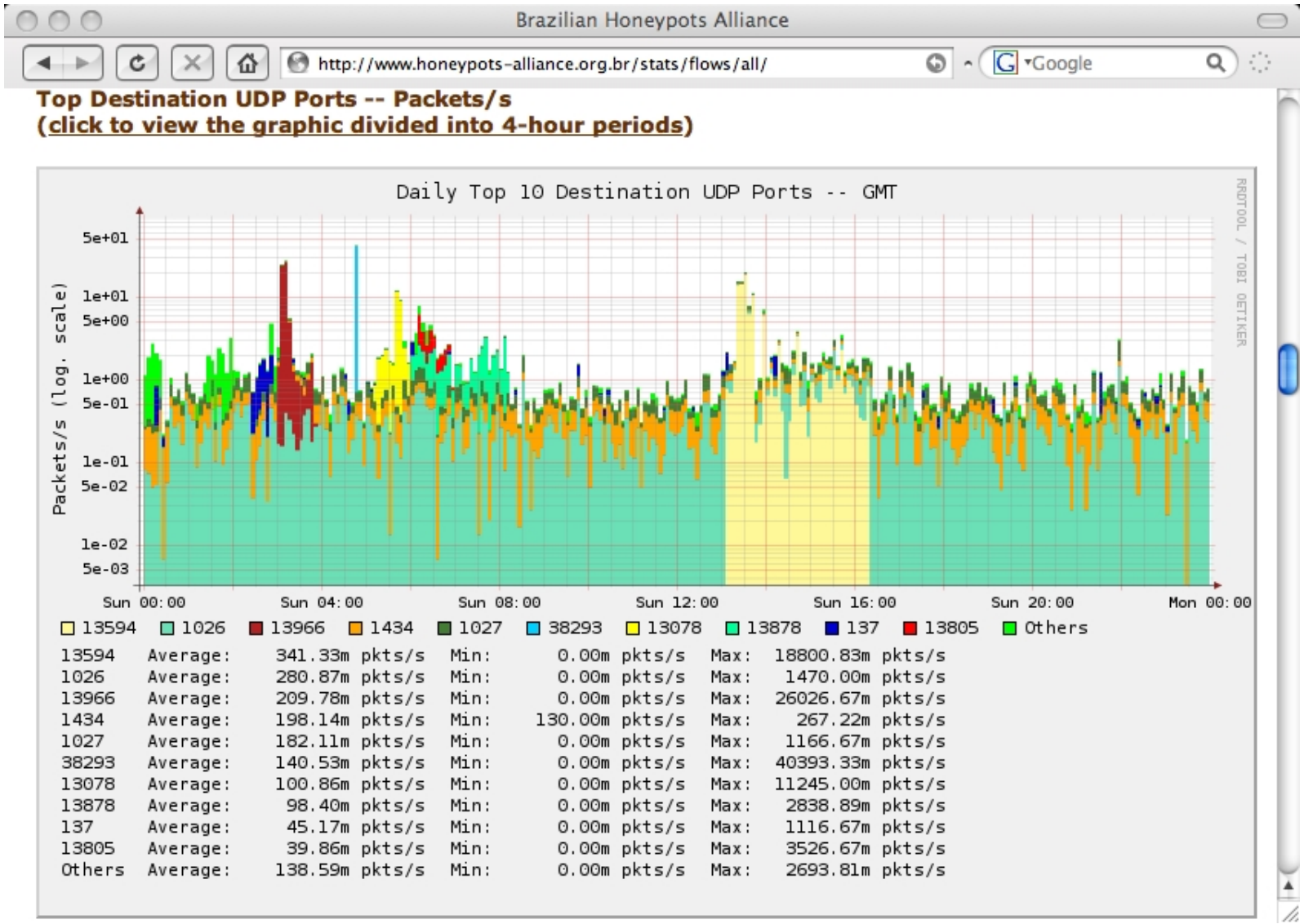
- Coleta e armazena os dados brutos contendo o tráfego de rede dos *honeypots*
  - inicia as conexões e usa `ssh` para transferir os dados OpenSSH - `http://www.openssh.org/`
- Realiza verificações de *status* em todos *honeypots*
  - *daemons*, sincronia de relógio, espaço em disco, etc
- Transfere as estatísticas geradas para o servidor *Web*
- Gera os e-mails de notificação
  - ferramentas usadas: `make`, `sh`, `perl`, `tcpdump`, `ngrep` (modificado), `jwhois`

Estatísticas Públicas - *Flows* TCP



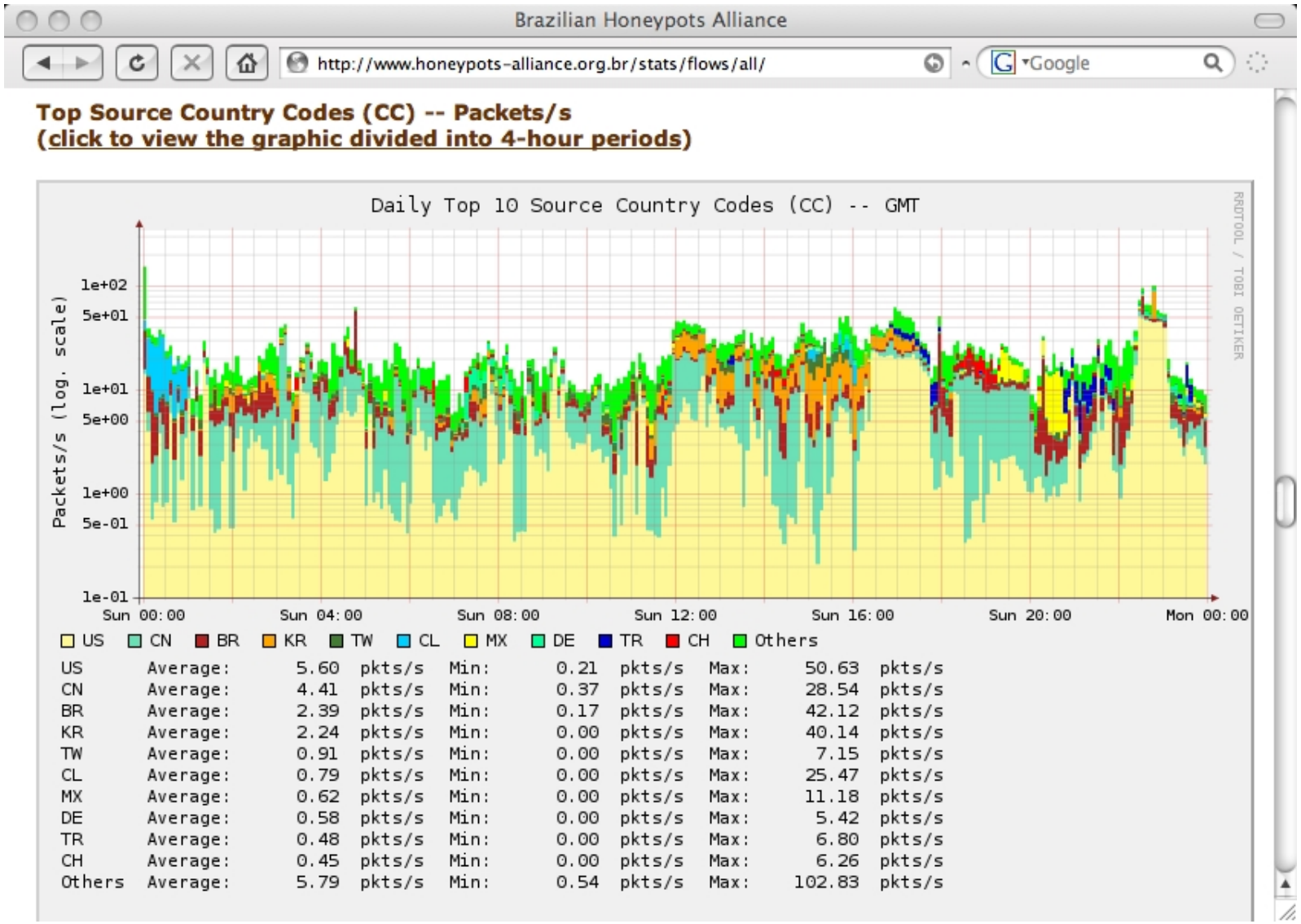
http://www.honeypots-alliance.org.br/stats/flows/all/

Estatísticas Públicas - *Flows* UDP



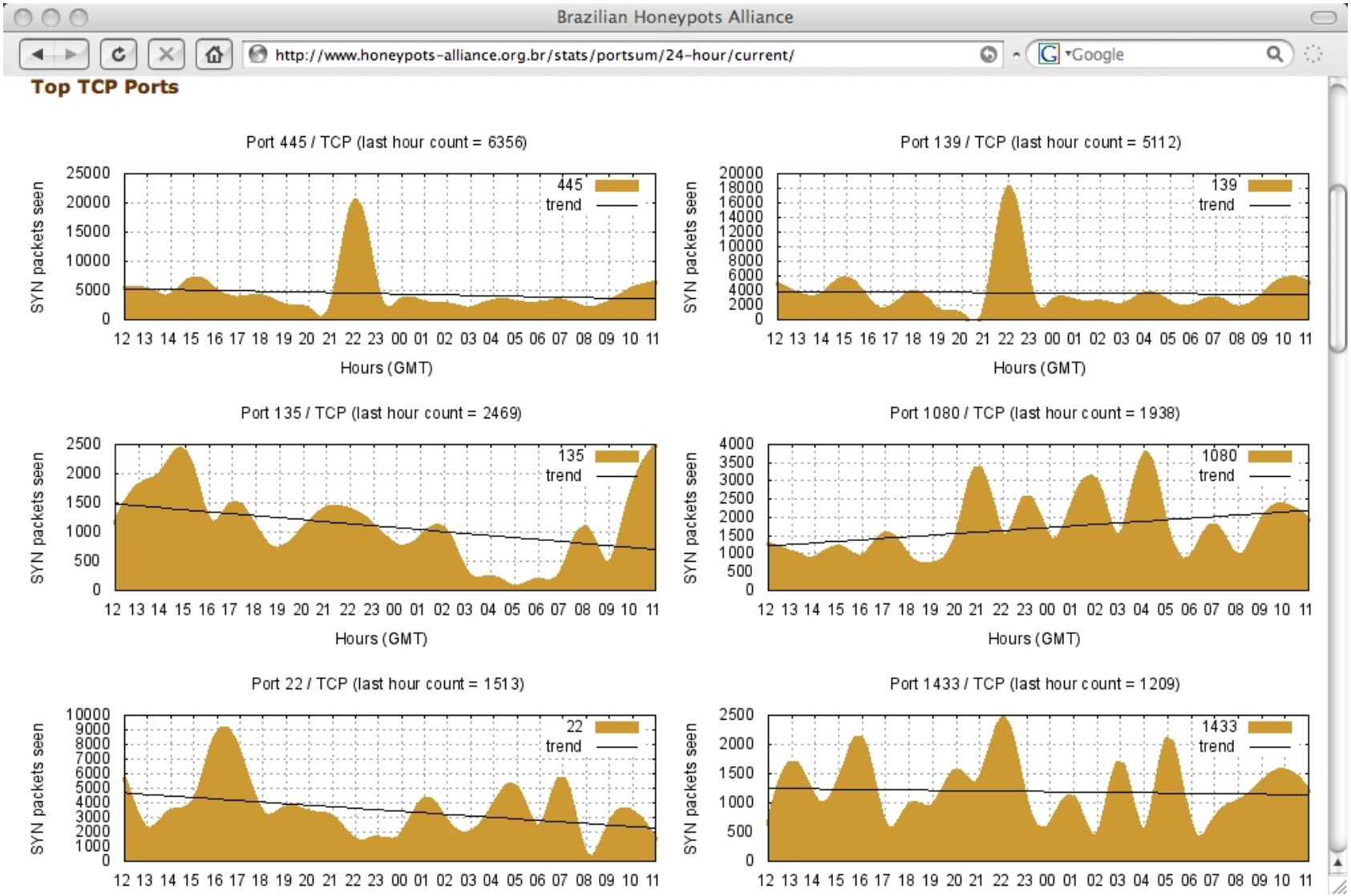
http://www.honeypots-alliance.org.br/stats/flows/all/

Estatísticas Públicas - *Flows* SO



http://www.honeypots-alliance.org.br/stats/flows/all/

Estatísticas Públicas - Tendências



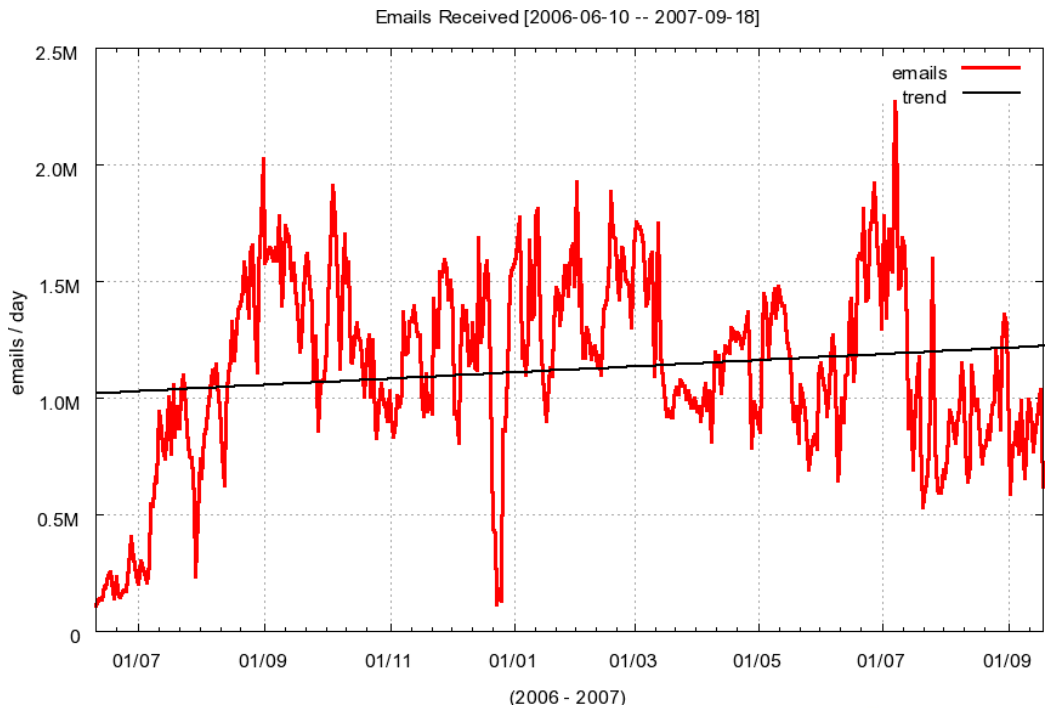
http://www.honeypots-alliance.org.br/stats/portsum/24-hour/current/

Projeto SpamPots

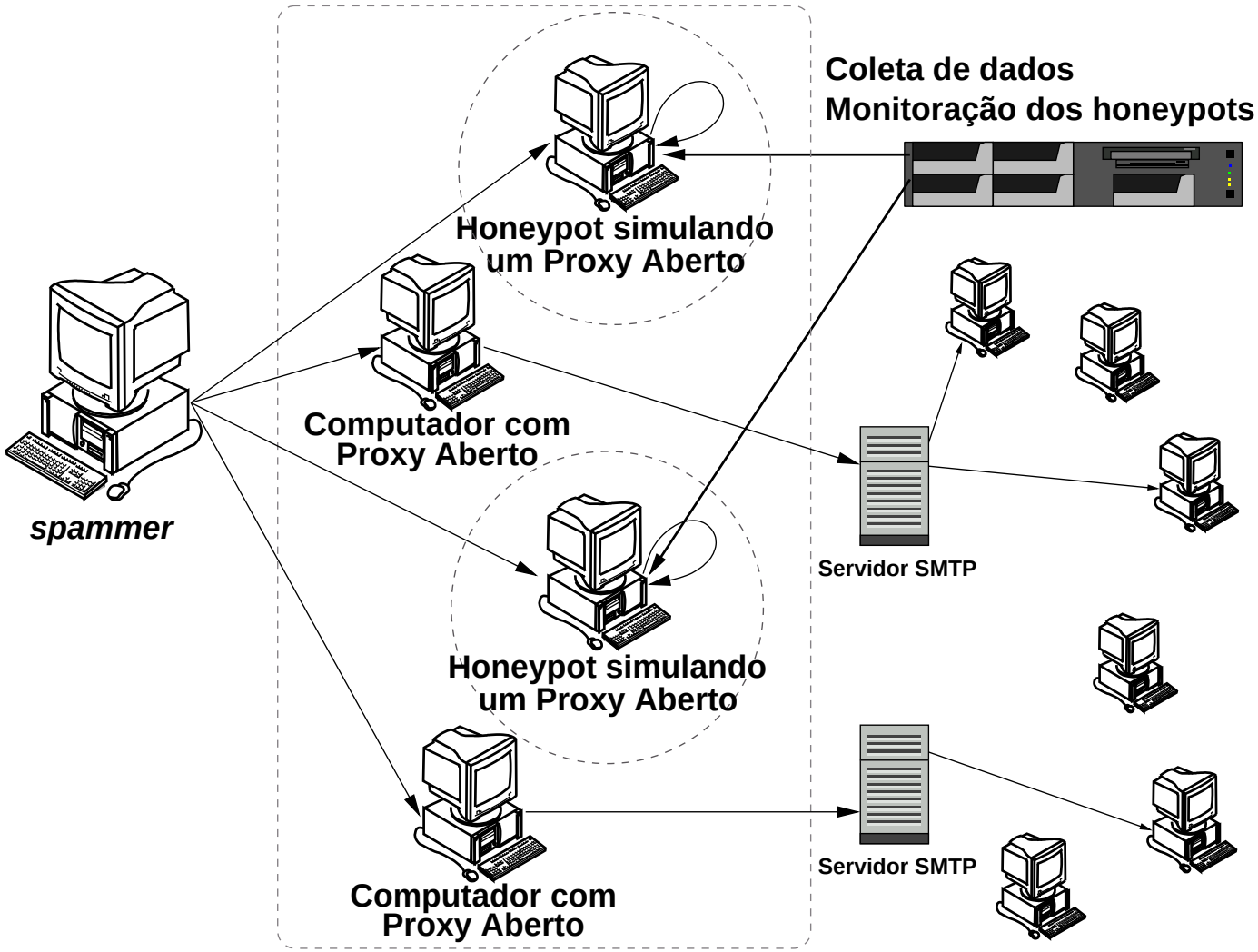
Métricas sobre o Abuso de Redes de Banda Larga para o Envio de *Spam*

- Mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- 10 *honeypots* de baixa interatividade
  - 5 operadoras diferentes de cabo e DSL
  - em conexões residenciais e comerciais

Período de coleta	**10/06/2006 a 18/09/2007**
Dias coletados	**466**
Total de *emails*	**524.585.779**
***Emails*/dia**	**1,2 milhões**
Destinatários	**4.805.521.964**
Destinatários/*spam*	**9,16**
IPs únicos	**216.888**
ASNs únicos	**3.006**
Country Codes	**165**



Arquitetura



http://www.cert.br/docs/whitepapers/spampots/

Configuração dos *Honeypots* (1/2)

OpenBSD: sistema operacional (SO) adotado

- número de problemas de segurança extremamente baixo, se comparado com outros SOs
- ciclo de atualizações bem definido (2x ao ano)
- boas características proativas de segurança
  - W^X, ProPolice, systrace, *random lib loading order*
- filtro de pacotes pf: *stateful*, *queueing* (ALTQ), redireção de pacotes
- logs no formato `libpcap`: permite *fingerprinting* passivo

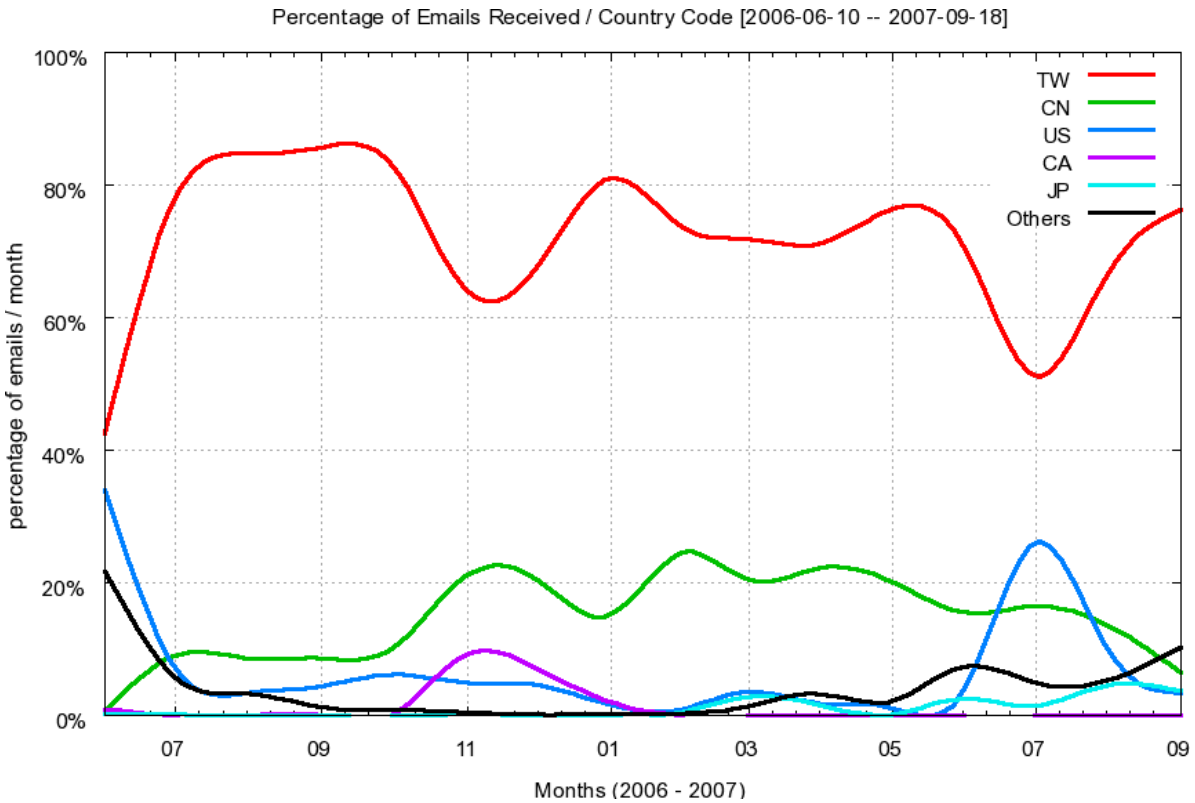
Configuração dos *Honeypots* (2/2)

Honeyd: emulação de serviços

- emulador de SMTP e *proxy* HTTP desenvolvidos por Niels Provos (com pequenas modificações)
- emulador de SOCKS 4/5 desenvolvido pela nossa equipe
  - simula a conexão com o servidor SMTP destino e passa a receber os *e-mails*
  - não entrega os *e-mails*

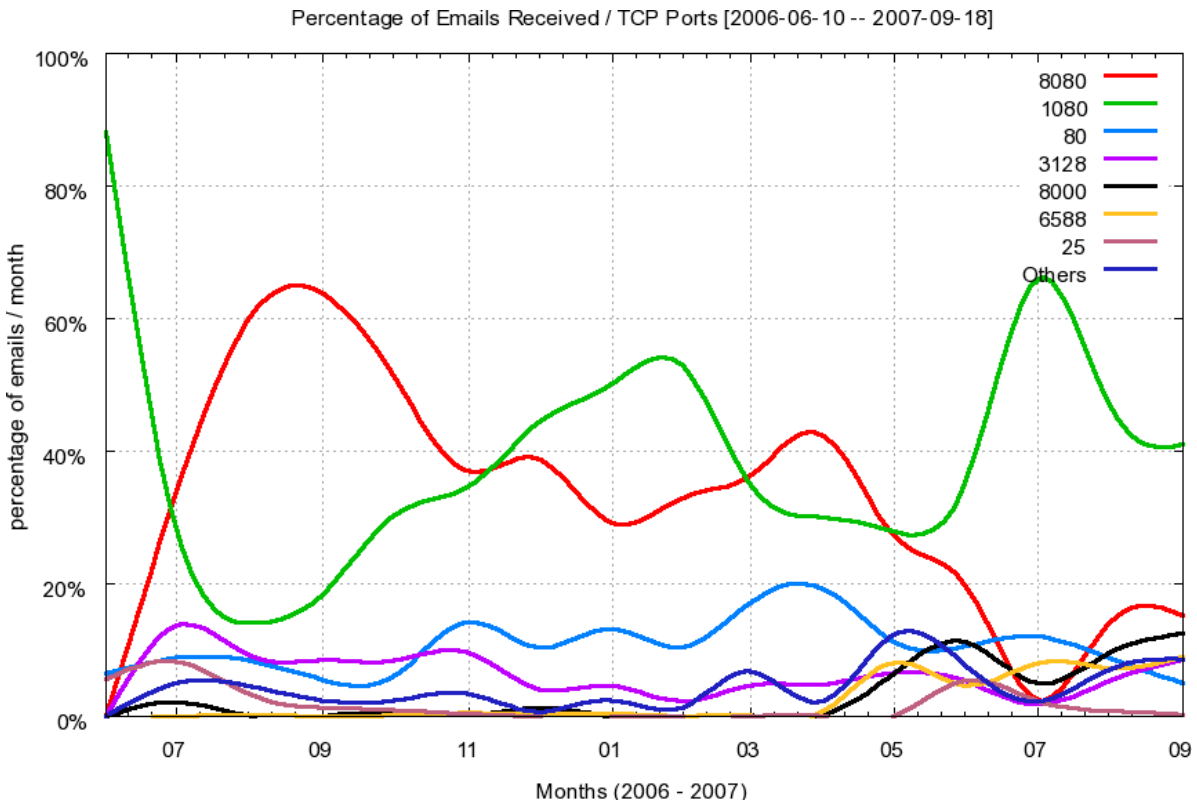
Resultados – *Country Codes* (CCs)

#	CC	Emails	%
01	TW	385.189.756	73,43
02	CN	82.884.642	15,80
03	US	29.764.293	5,67
04	CA	6.684.667	1,27
05	JP	5.381.192	1,03
06	HK	4.383.999	0,84
07	KR	4.093.365	0,78
08	UA	1.806.210	0,34
09	DE	934.417	0,18
10	BR	863.657	0,16



Resultados – Portas Abusadas

Porta	Protocolo	Serviço	%
1080	SOCKS	socks	37,31
8080	HTTP	http	34,79
80	HTTP	http	10,92
3128	HTTP	Squid	6,17
8000	HTTP	http	2,76
6588	HTTP	AnalogX	2,29
25	SMTP	smtp	1,46
4480	HTTP	Proxy+	1.38
3127	SOCKS	MyDoom	1,00
3382	HTTP	Sobig.f	0,96
81	HTTP	http	0,96



Referências

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