Implementação de uma Rede de Honeypots Distribuídos Utilizando OpenBSD e Ferramentas de Software Livre

Marcelo H. P. C. Chaves

mhp@cert.br

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

NIC.br – Núcleo de Informação e Coordenação do Ponto br

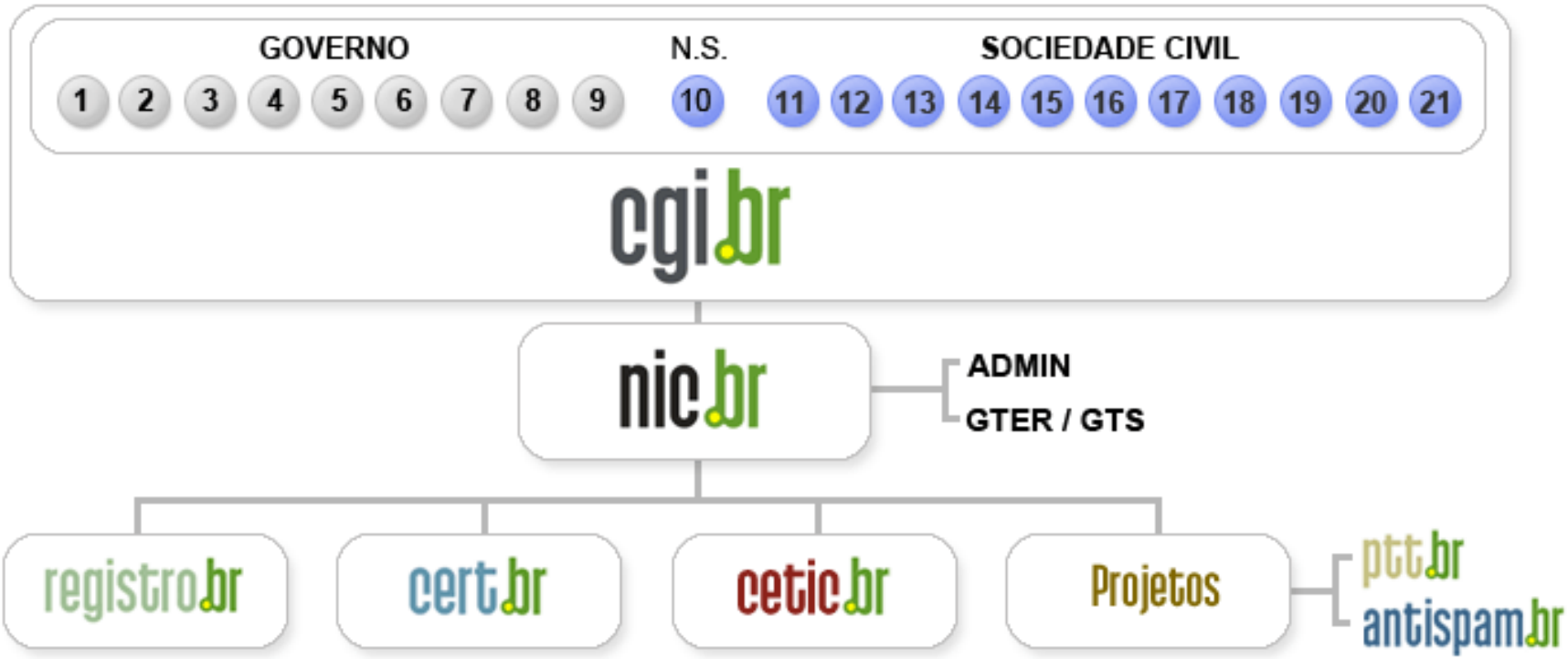
CGI.br – Comitê Gestor da Internet no Brasil

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**

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

CERT.br

Criado em 1997 para receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira, exercendo as seguintes funções:

- Ser um ponto de contato nacional para notificação de incidentes de segurança
- Prover a coordenação e o apoio necessário no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades
- Auxiliar novos CSIRTs a estabelecerem suas atividades
- Prover treinamento na área de tratamento de incidentes
- Produzir documentos de boas práticas
- Aumentar a conscientização sobre a necessidade segurança na Internet

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

Agenda

- Histórico
- Motivação
- O Projeto
  - Arquitetura
  - Instituições Consorciadas
  - Requisitos
- Estatísticas e Uso dos Dados
- Desafios para Implantar e Manter a Rede
- Benefícios e Desvantagens
- Trabalhos Futuros
- Referências

Breve Histórico

- Março/2002
  - Primeira *honeynet* do Projeto Honeynet.BR implantada
- Junho/2002
  - Projeto Honeynet.BR passa a fazer parte da *Honeynet Research Alliance*
- Setembro/2003
  - O “Consórcio Brasileiro de Honeypots – Projeto Honeypots Distribuídos” é iniciado

Motivação

- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro
- Sensores geograficamente distribuídos pelo país
  - em diversos locais e cobrindo vários ASNs
- Dados úteis no processo de resposta a incidentes

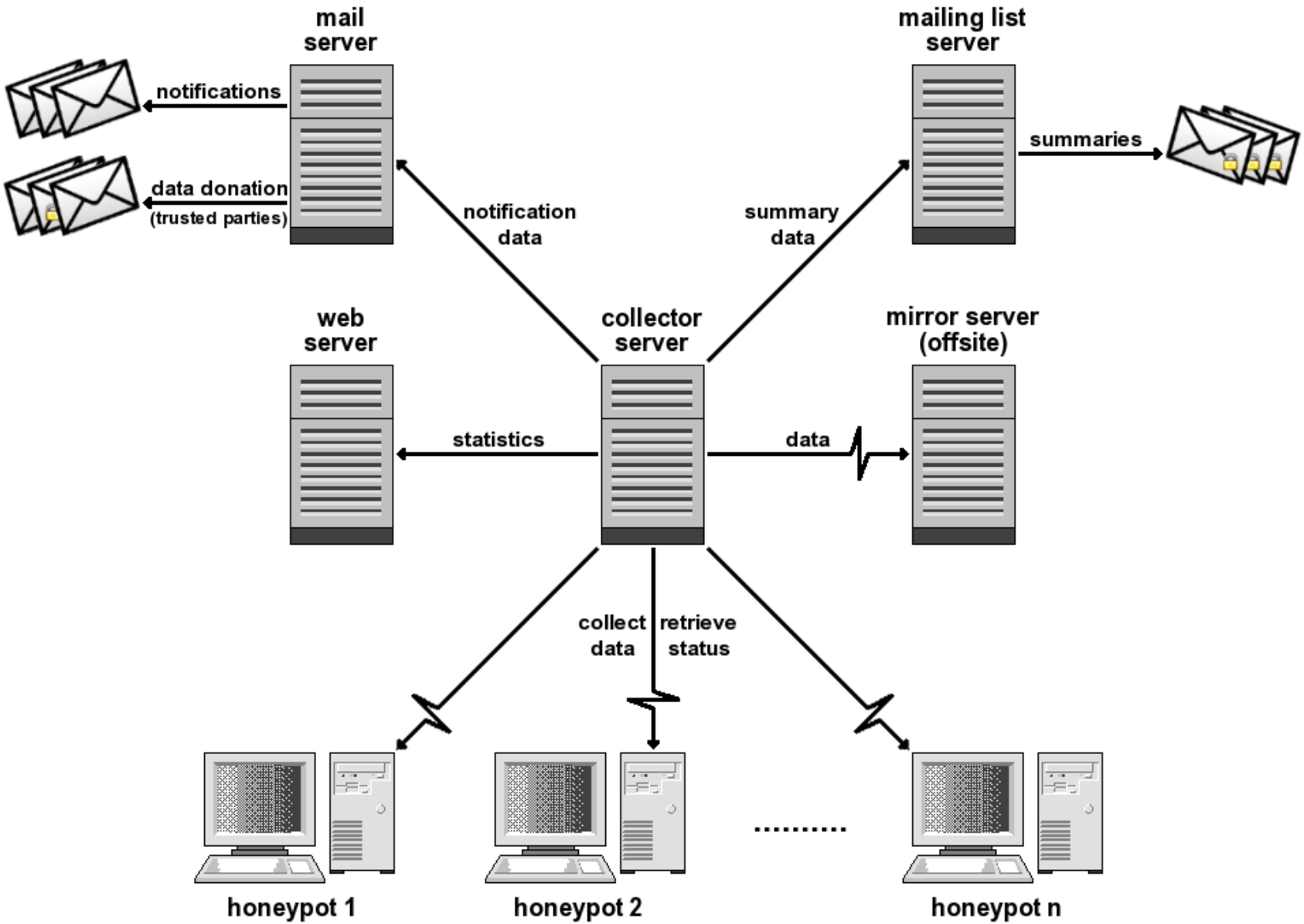
O Projeto

Consórcio Brasileiro de Honeypots

Projeto Honeypots Distribuídos

- Coordenação: CERT.br e CenPRA
- Uso de *honeypots* de baixa interatividade
- Baseado no trabalho voluntário das instituições consorciadas

Arquitetura



Honeypots de Baixa Interatividade

- **OpenBSD** – o Sistema Operacional (SO) adotado
  - familiaridade
  - número de furos de segurança extremamente baixo, se comparado com outros SOs
  - boas características proativas de segurança
    - W^X, ProPolice, systrace, *random lib loading order*
  - ciclo de atualizações bem definido (2x ao ano)
  - fornecido para várias plataformas
    - i386, sparc, sparc64, amd64, etc
  - um dos melhores filtros de pacotes gratuitos
    - *stateful*, *redundancy*, *queueing* (ALTQ), etc
  - *logs* de *firewall* no formato `libpcap`

http://www.openbsd.org/

Honeypots de Baixa Interatividade (2)

- **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*
  - Outos 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 verificacões 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`
- Todos os dados são copiados para o servidor *backup* (*offsite mirror*)

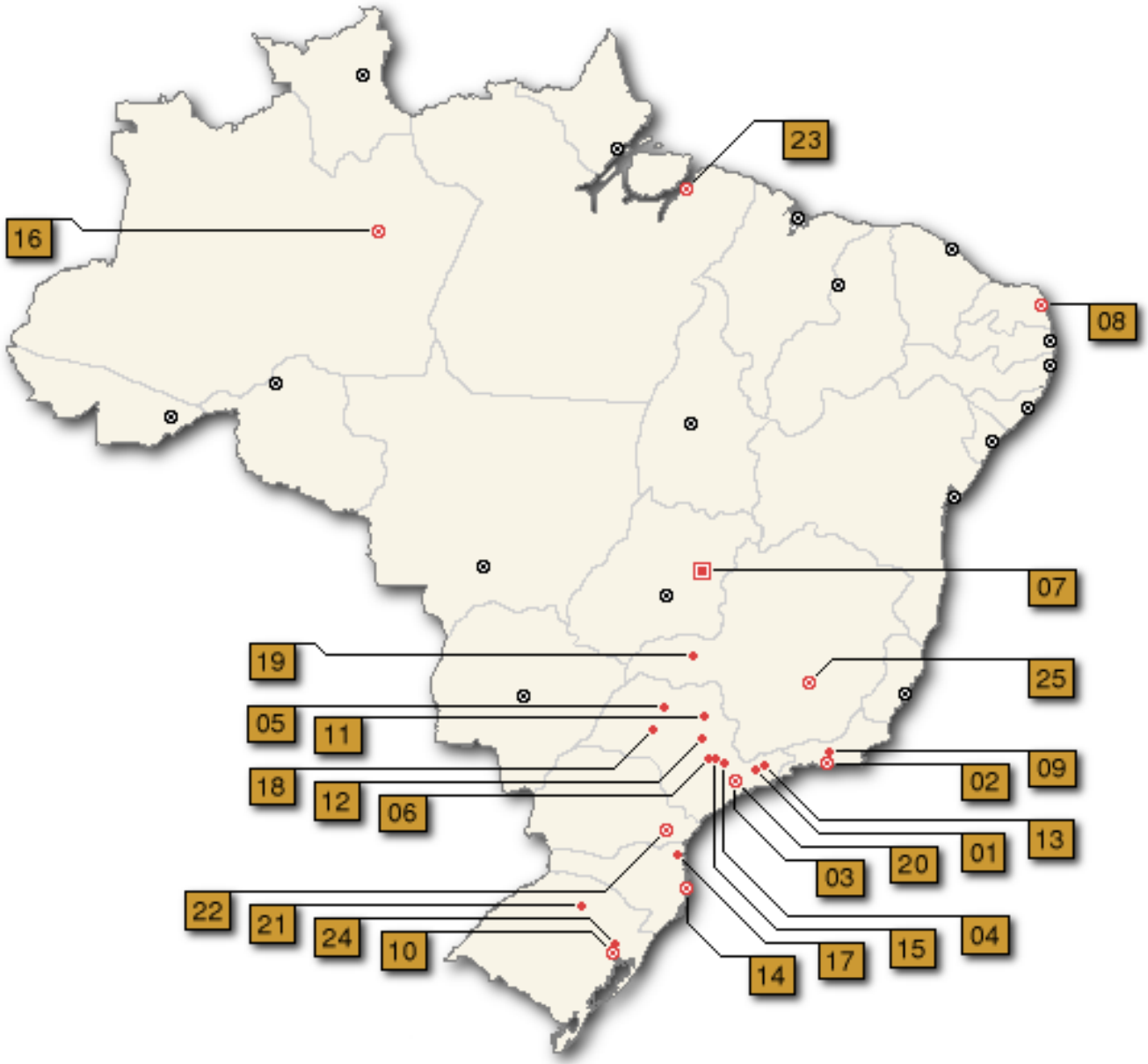
Instituições Consorciadas

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

Requisitos para a Instituição

- Seguir os padrões estipulados (SO, configuração segura, atualizações, etc)
- Não poluição dos dados
- Permitir todo o tráfego de/para o(s) *honeypot(s)*
- Não fornecer endereço IP e rede associada
  - estas informações devem ser sanitizadas
- Não coletar tráfego de redes de produção
- Não trocar informações abertamente (sem criptografia)

Cidades onde os *Honeypots* estão Localizados



As 37 Instituições do Consórcio

#	Cidade	Instituiição
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, UOL, USP
04	Campinas	CenPRA, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministério da Justiça, TCU, UNB LabRedes
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR, PUCPR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

Estatísticas
e Uso dos Dados

Estatísticas Exclusivas p/ Membros

- Sumários de cada *honeypot*
  - total de pacotes
  - pacotes UDP/TCP/ICMP e Outros
  - quantidade de dados brutos capturados
  - Países mais freqüentes (dados de alocação IP)
  - SOs, IPs e portas mais freqüentes
- Um sumário combinado de todos *honeypots*
- Correlacionamentos
  - portas/IPs vistos em mais de 30% dos *honeypots*
- Ferramentas usadas:
  - `sh`, `perl`, `tcpdump (OS fingerprinting)`, `gpg`

Estatísticas Exclusivas p/ Membros (2)

- Números no sumário de 1 dia (exemplo)

Total de pacotes	21.455.939
Qtde de dados brutos	573,9MB (comprimido)

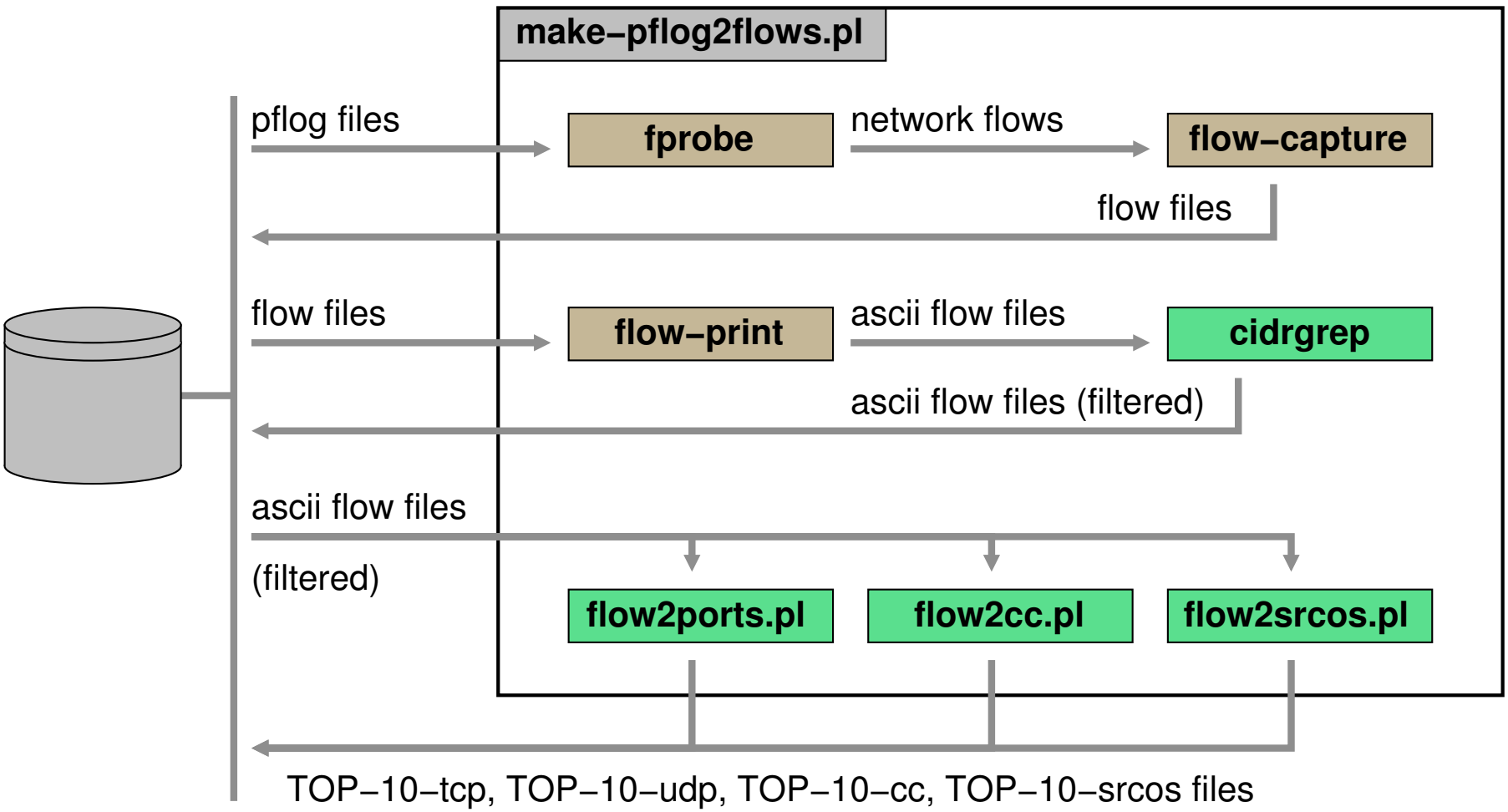
Protocolo	Número de Pacotes	IPs Únicos
TCP	20.420.621 (95,17%)	30.802
UDP	240.530 (01,12%)	7.488
ICMP	785.734 (03,66%)	14.712
Outros	9.054 (00,04%)	—

Estatísticas Públicas

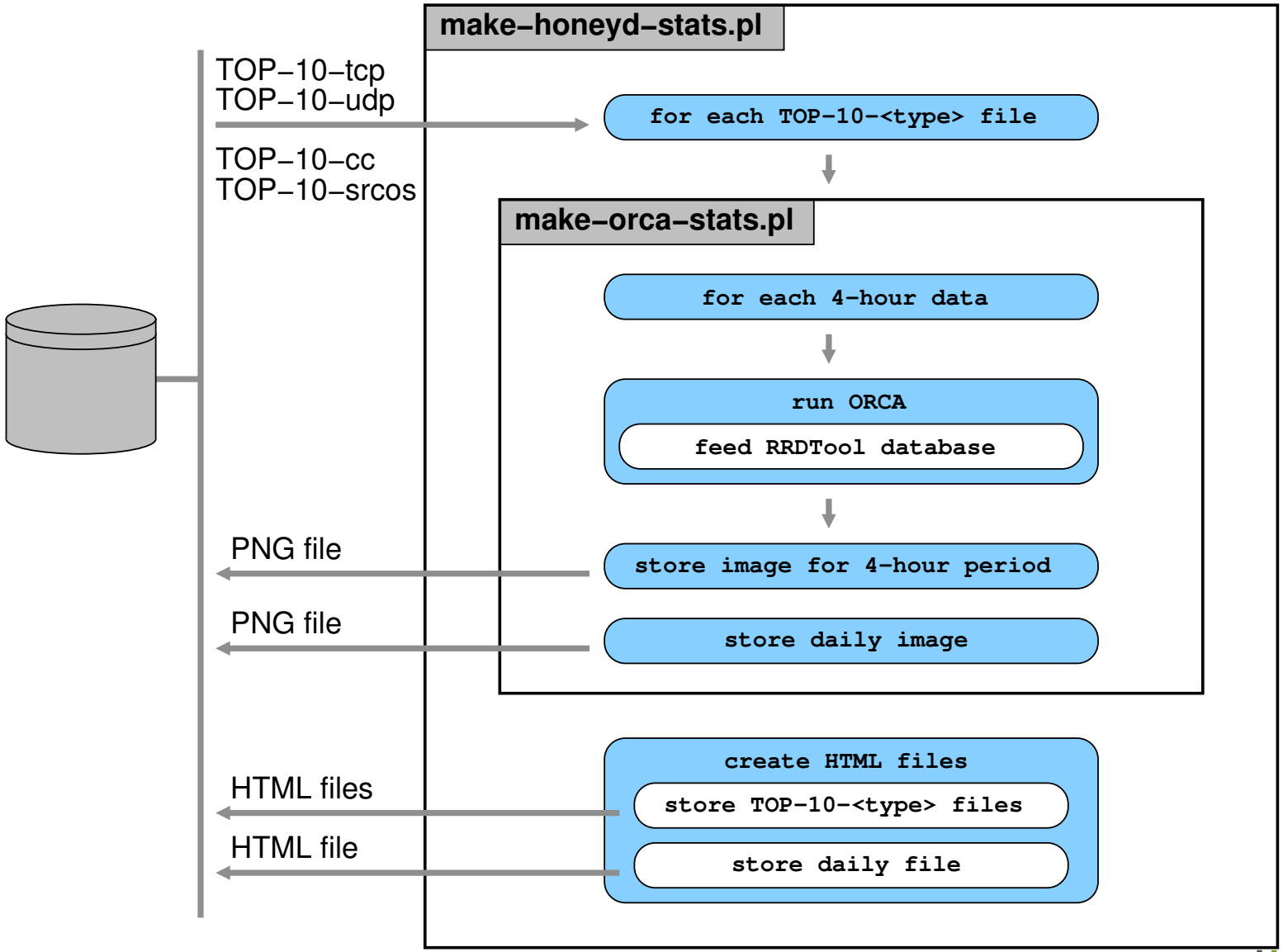
- Fluxos extraídos dos dados coletados em todos os *honeypots*
  - SOs, portas TCP/UDP e países mais freqüentes
  - pacotes/s e bytes/s
  - diário e em períodos de 4 horas
- Ferramentas usadas:
  - `perl`, `tcpdump (OS fingerprinting)`, `fprobe`, `flow-tools`, `RRDtool`, `Orca`
- Disponíveis em:

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

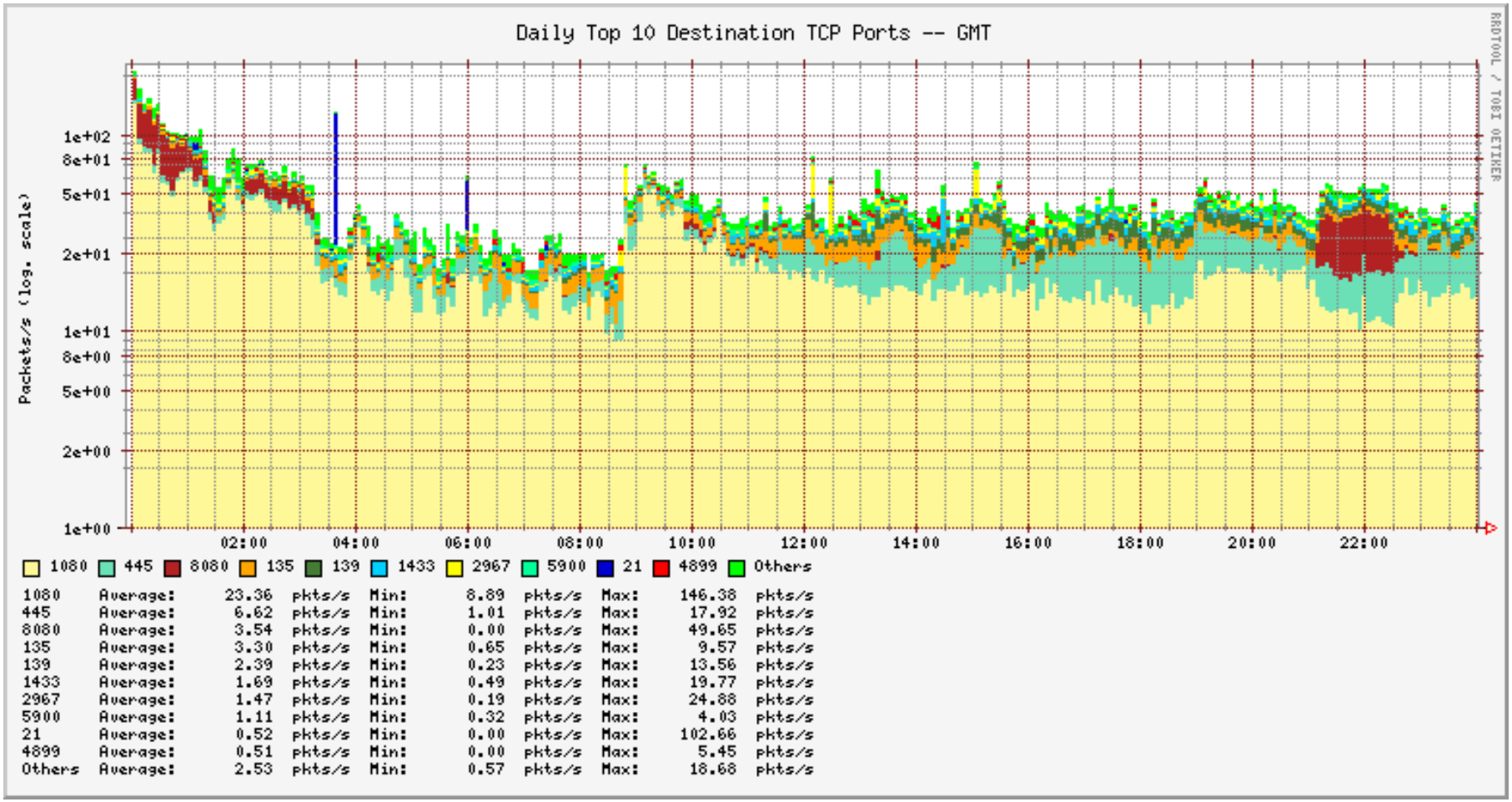
Geração das Estatísticas Públicas



Geração das Estatísticas Públicas (2)

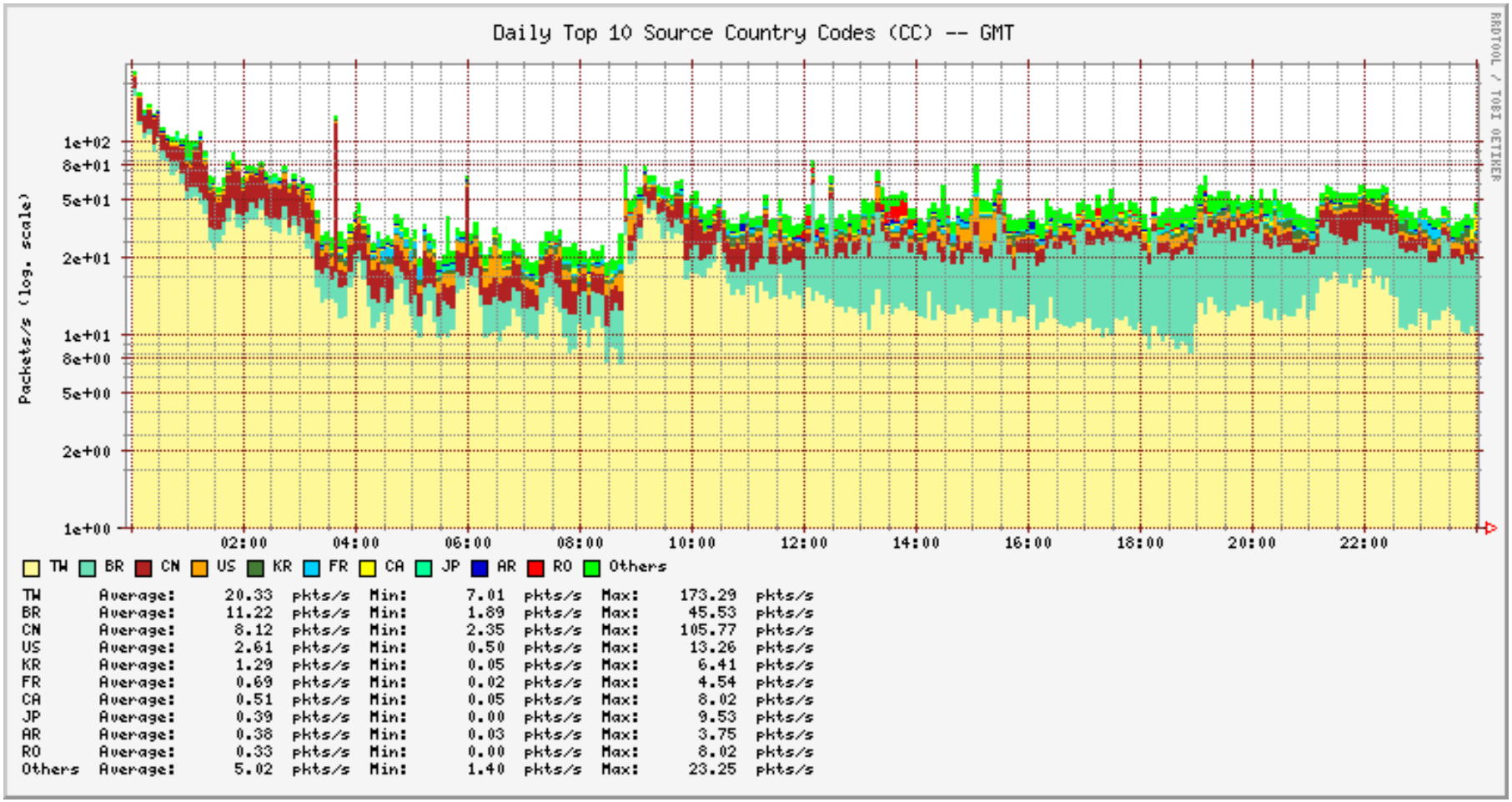


Estatísticas Públicas (fluxos): *Top TCP Ports*



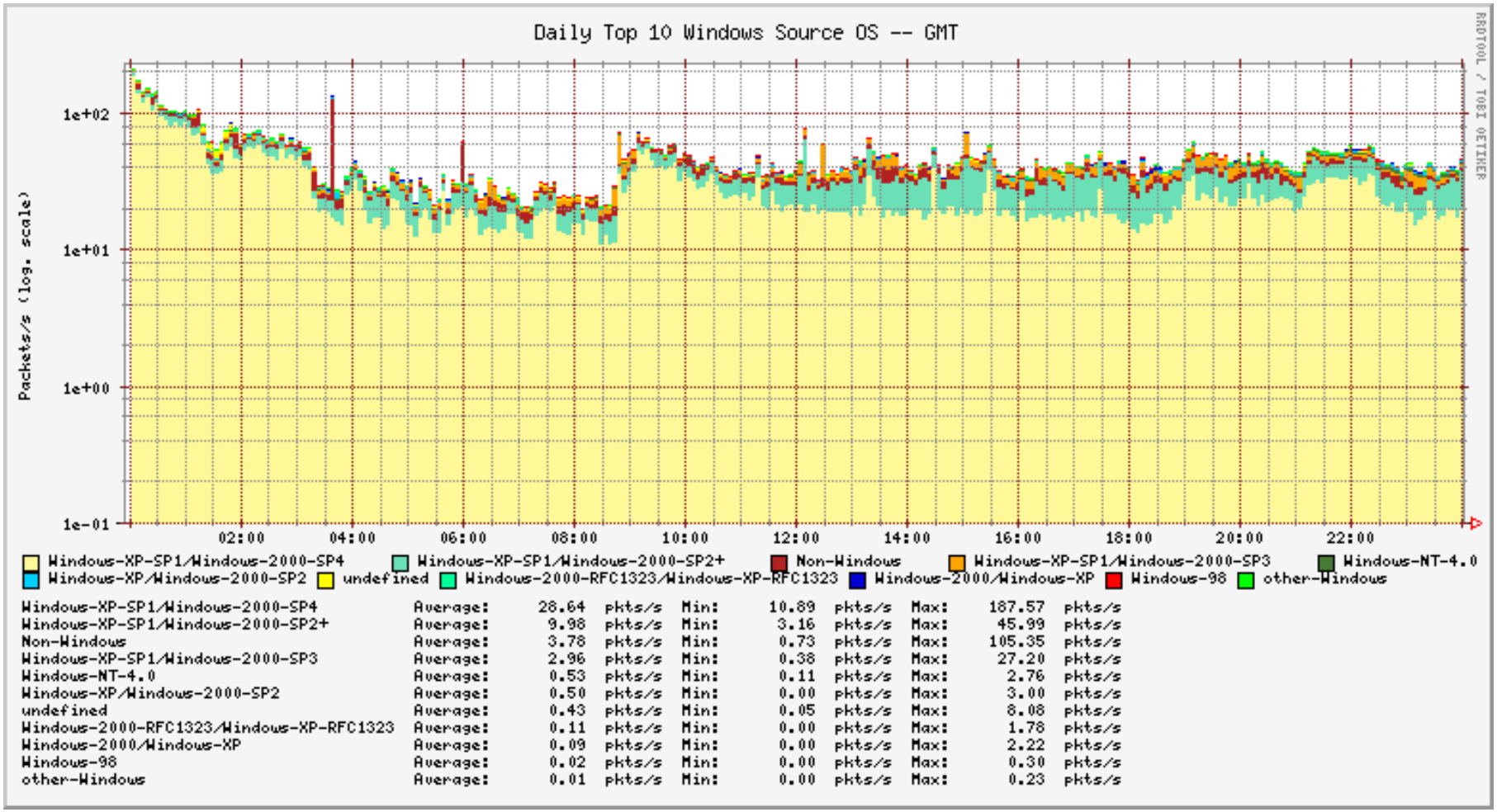
29 de março de 2007 – http://www.honeypots-alliance.org.br/stats/

Estatísticas Públicas (fluxos): *Top CC*



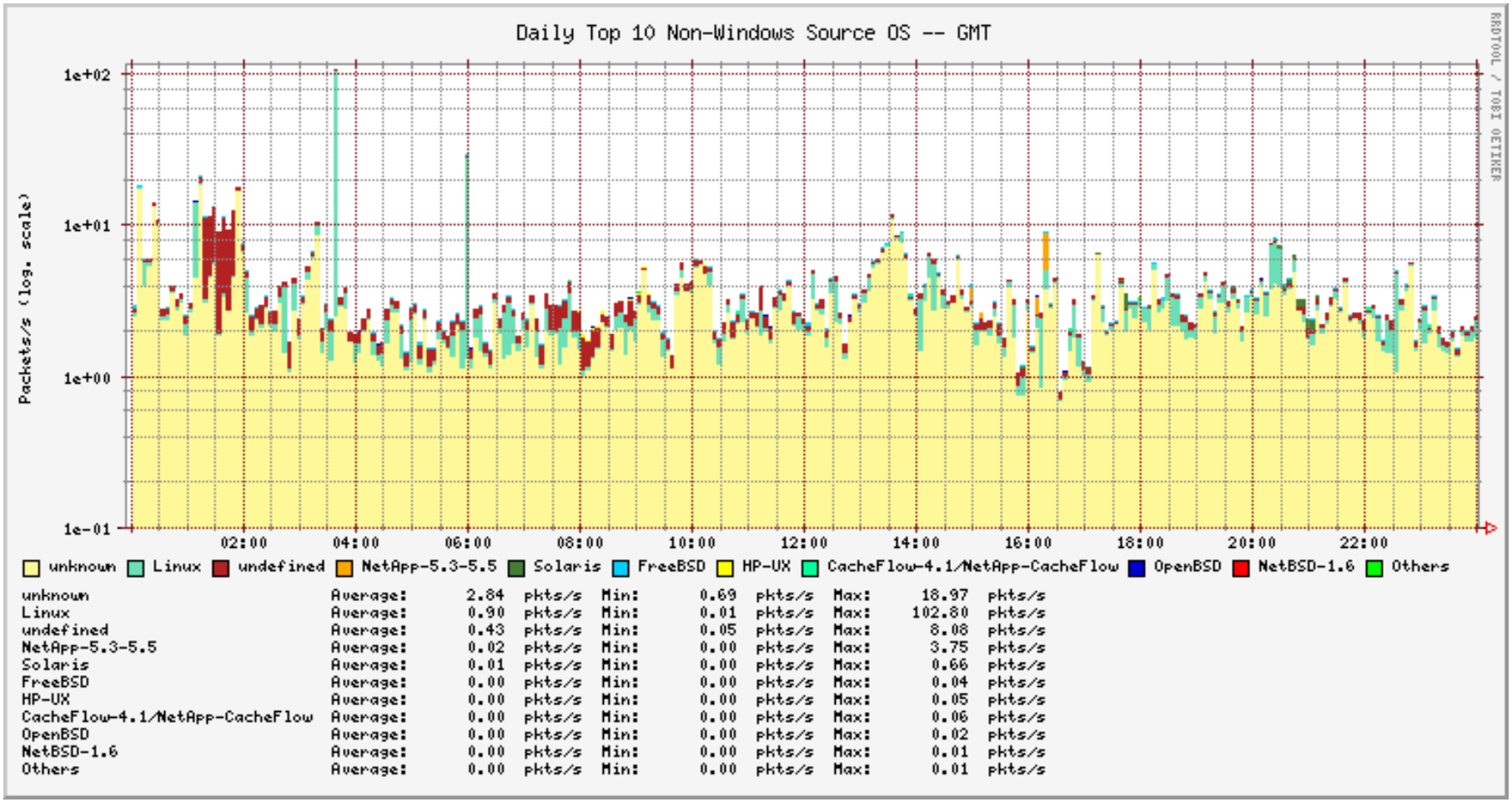
29 de março de 2007 – http://www.honeypots-alliance.org.br/stats/

Estatísticas Públicas (fluxos): *Top Win Src.OS*



29 de março de 2007 – http://www.honeypots-alliance.org.br/stats/

Estatísticas Públicas (fluxos): *Top Non-Win Src.OS*

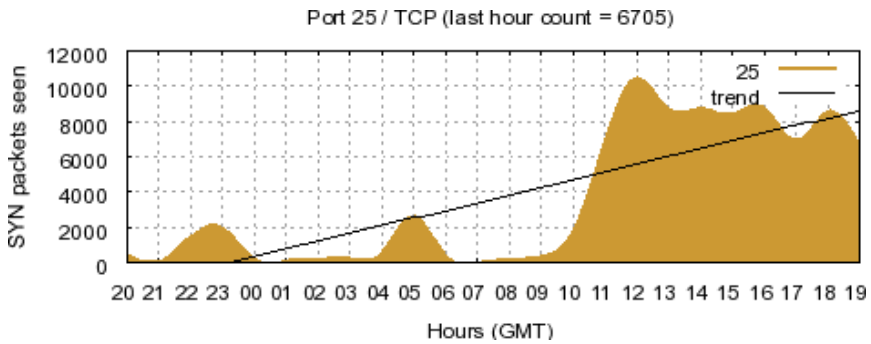


29 de março de 2007 – http://www.honeypots-alliance.org.br/stats/

Estatísticas Públicas: *Port Summary* (em breve)

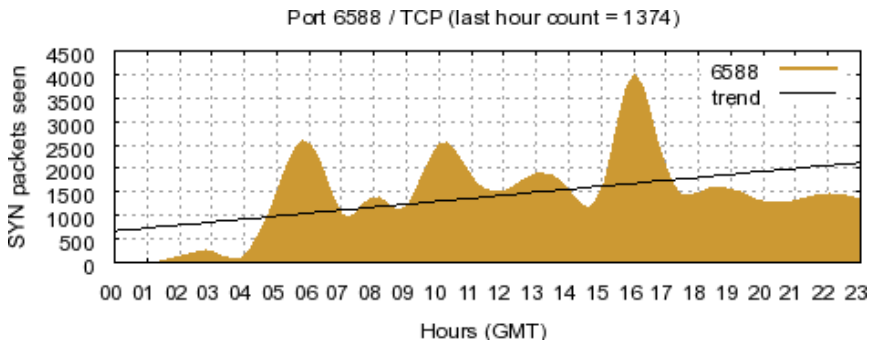
- Horária

19: 2007-04-08 20:00 – 2007-04-09 19:59 (GMT)



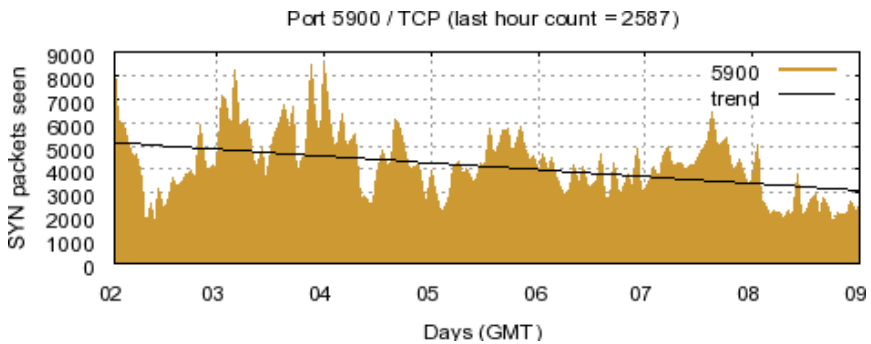
- Diária

08: 2007-04-08 00:00 – 2007-04-08 23:59 (GMT)



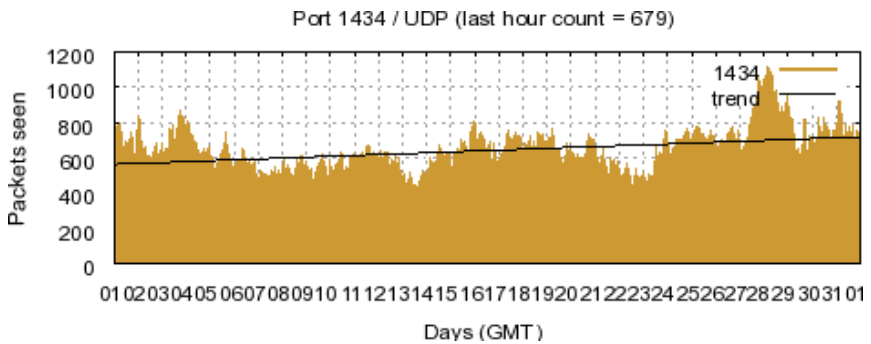
- Semanal

14: 2007-04-02 00:00 – 2007-04-08 23:59 (GMT)



- Mensal

03: 2007-03-01 00:00 – 2007-03-31 23:59 (GMT)



Ferramentas usadas: `sh`, `perl`, `gnuplot`

Uso dos Dados

- Instituições Consorciadas
  - observação de tendências e varreduras por novas vulnerabilidades
  - detecção imediata:
    - aparecimento de novos *worms*/*bots*, máquinas comprometidas, erros de configuração de rede
- Resposta a incidentes (CERT.br)
  - identificação de atividades notadamente maliciosas/abusivas
    - *worms*, *bots*, varreduras, *spam* e *malware* em geral
  - notificações para os contatos de redes brasileiras
    - incluindo dicas de recuperação
  - doação dos dados coletados, relacionados a outros países, para parceiros

Desafios para Implantar e Manter a Rede

Desafios para Encontrar Instituições

Como encontrá-las

- Outros grupos de resposta a incidentes (CSIRTs)
- Reportadores de incidentes conhecidos
- Participantes dos nossos cursos
- Pessoas indicadas pelas instituições já consorciadas

Depois de encontrá-las, precisamos convencê-las

- Por que devem colocar um *honeypot* em suas redes?
- Que vantagens têm ao compartilhar os dados conosco?

Pontos Importantes: alcançar/manter a Instituição

Não estamos oferecendo uma “caixa preta”

- Elas têm acesso aos seus *honeypots*
- Elas podem estender a configuração do *honeypot*

O *honeypot* não captura dados de redes de produção

- apenas dados direcionados ao *honeypot* são coletados

Elas podem usar os dados livremente

- Por exemplo, como complemento de seus IDSs, etc

Nós fornecemos informações exclusivas para as instituições

- Sumários diários (sanitizados) – cada *honeypot*, combinado, correlações

Informações trocadas em uma lista criptografada

Desafios para Manter o Projeto

Depende da cooperação das instituições para manter e atualizar os *honeypots*

- mais difícil de manter do que um *honeypot* "*plug and play*"

O projeto se torna mais difícil de gerenciar à medida que o número de *honeypots* cresce

- Mais pessoas para coordenar
- Mais recursos necessários (espaço em disco, banda, etc)
- Questões de gerenciamento de chaves PGP
- Alguns *honeypots* começam a apresentar problemas de *hardware*

Benefícios do Projeto e Desvantagens da Arquitetura

Benefícios

Curto Prazo

- Poucos falso positivos, baixo custo e baixo risco
- Notificações de redes originando atividades maliciosas e produção de estatísticas
- Capacidade de coletar exemplares de *malware*
  - *listeners* devenvolvidos para: `mydoom`, `subseven`, `socks`, `ssh`, `etc`.

Longo Prazo

- Permite que os membros aperfeiçoem seus conhecimentos em diversas áreas:
  - *honeypots*, *firewall*, *OS hardening*, PGP, *intrusion detection*, etc
- Melhora no relacionamento entre o CERT.br e as instituições consorciadas

Desvantagens da Arquitetura

- *Honeypots*, normalmente, não observam ataques direcionados à redes de produção
- As informações coletadas são limitadas se comparadas às coletadas em *honeypots* de alta interatividade

Trabalhos Futuros e Referências

Trabalhos Futuros

- Dar continuidade na expansão da rede
  - 2 novas instituições em fase de instalação
  - 5 instituições candidatas
- Fornecer outras estatísticas públicas:
  - mensal, semanal, diária e horária
- Mais investimentos em *spam traps*

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- CGI.br – Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- CERT.br
  http://www.cert.br/
- Consórcio Brasileiro de Honeypots – Projeto Honeypots Distribuídos
  http://www.honeypots-alliance.org.br/
- Honeynet.BR
  http://www.honeynet.org.br/
- Apresentações anteriores sobre o Projeto
  http://www.honeynet.org.br/presentations/
- *Honeypots* e *Honeynets*: Definições e Aplicações (*white paper*)
  http://www.cert.br/docs/whitepapers/honeypots-honeynets/