Honeynet: atualização e tendências

João Ceron
Liane Tarouco
Leandro Bertholdo

Sumário

- Introdução
- Objetivos
- Metodologia
- Cenário
- Análise de resultados
- Conclusões

Introdução

- Propagação automática de malwares (*background noise*)
  - Scanner ssh
  - Bot
  - Worms

"Up to a quarter of the 6000 million machines connected to Internet may be used by criminals"

Vicent Cerf

BBC News 2007, Criminals may overwhelm the web

Introdução

- Honeypots
  - Honeynets
- Acesso a portas
- Observar padrões
- Ataques automatizados (worms,scanners,bots)

Objetivo

- Utilizar honeynet para traçar um panorama das sondagens
  - Informações dos exploits
  - Comportamento
  - padrões
- Automatizar detecção a nível de backbone de rede

Metodologia

- Implementar uma honeynet
  - vulnerabilidades
- Capturar binários que malwares
- Realizar uma análise a nível de sistema operacional (sandbox)
  - Analisar o *network-level behavior*
- Buscar padrão de rede obtido no *backbone* da rede (fluxos)

Metodologia

- Honeynet
  - Emulando um /24

```
ifconfig disc0 create
#!/bin/sh
    for i in `seq 254`; do
    echo "ifconfig disc0 200.X.X.$i netmask 255.255.255.0 alias"
    done;
```

Servidor FreeBSD - CPU 1Ghz – 512M de RAM

Metodologia

- Software nepenthes
- Total de 21 vulnerabilidades emuladas
- Armazenar binários

Port	Vulnerbility	Module
42	MS04-006	vuln_wins
80	MS04-045 MS03-007	vuln_asn1
	MS03-051	
	MS04-011	
135	MS03-039	vuln_dcom
139	MS04-012	vuln_netbiosname
	MS04-031	vuln_netdde
443		vuln_iis
445		vuln_asn1
	MS04-011	vuln_lsass
	MS04-012	vuln_dcom
	MS03-039	
1023		vuln_sasserftpd
1025		vuln_dcom

Metodologia

- Realizar uma análise a nível de sistema operacional (sandbox)
  - CWSandbox
    - Modificacoes no sistema de arquivo
    - Registro
    - Mutexes
    - Processos
    - Contas de usuários
    - Windows shares
    - DLLs
    - E outros

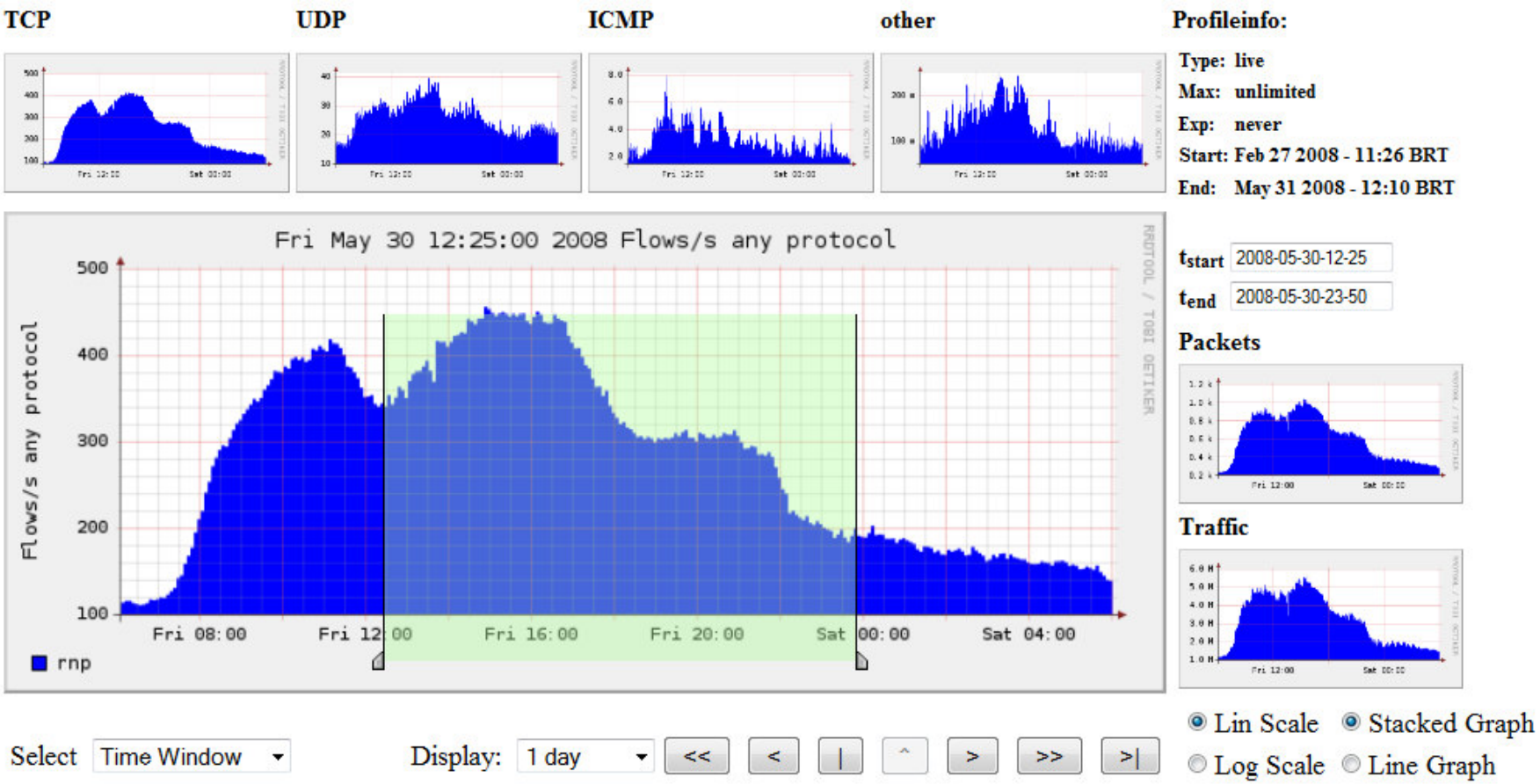
Metodologia

```
for i in `ls *`
do
    echo $i
    curl -F "email=return@tche.com" -F "upfile=@$i"
    "http://cwsandbox.org/submit.php?action=verify" >>
    /home/ceron/sandbox.txt
    printf "\n" >> /home/ceron/sandbox.txt
done
```

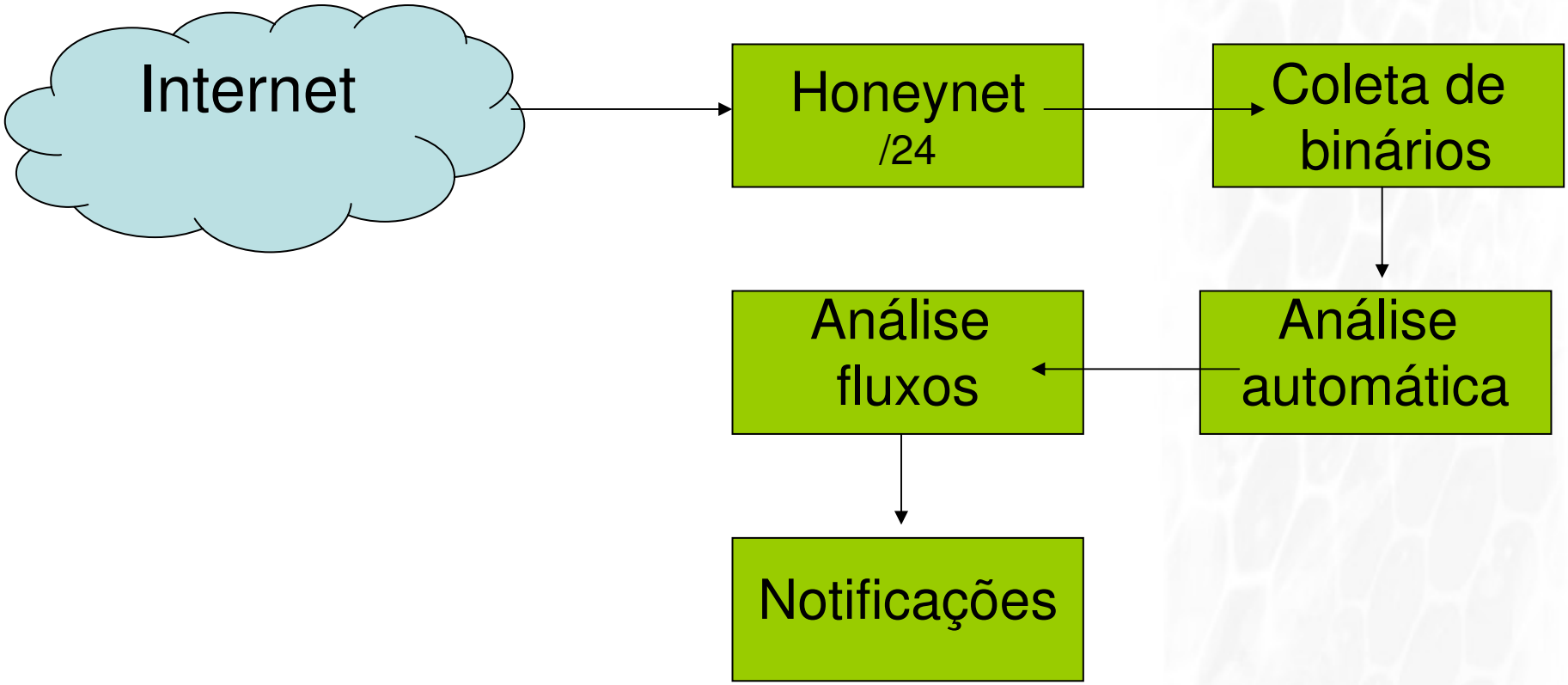
- URL dos relatórios
- Parser perl: padrões de rede

Análise dos resultados

- flows

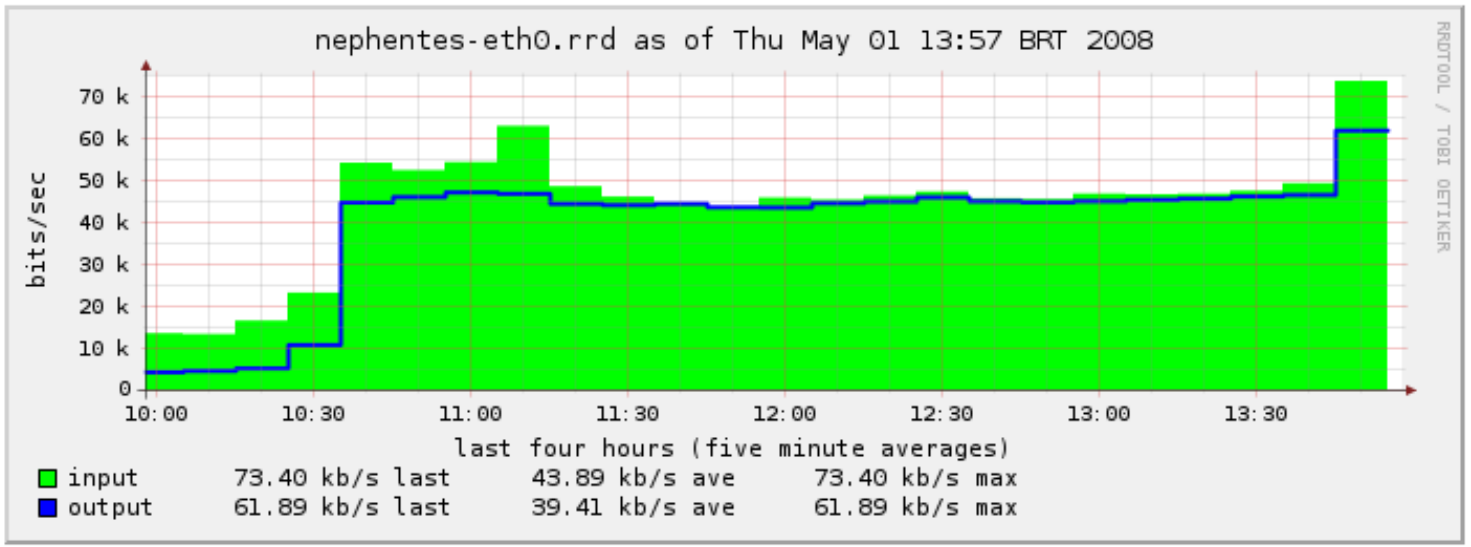


Cenário


Internet
Honeynet
/24
Coleta de
binários
Análise
automática
Análise
fluxos
Notificações

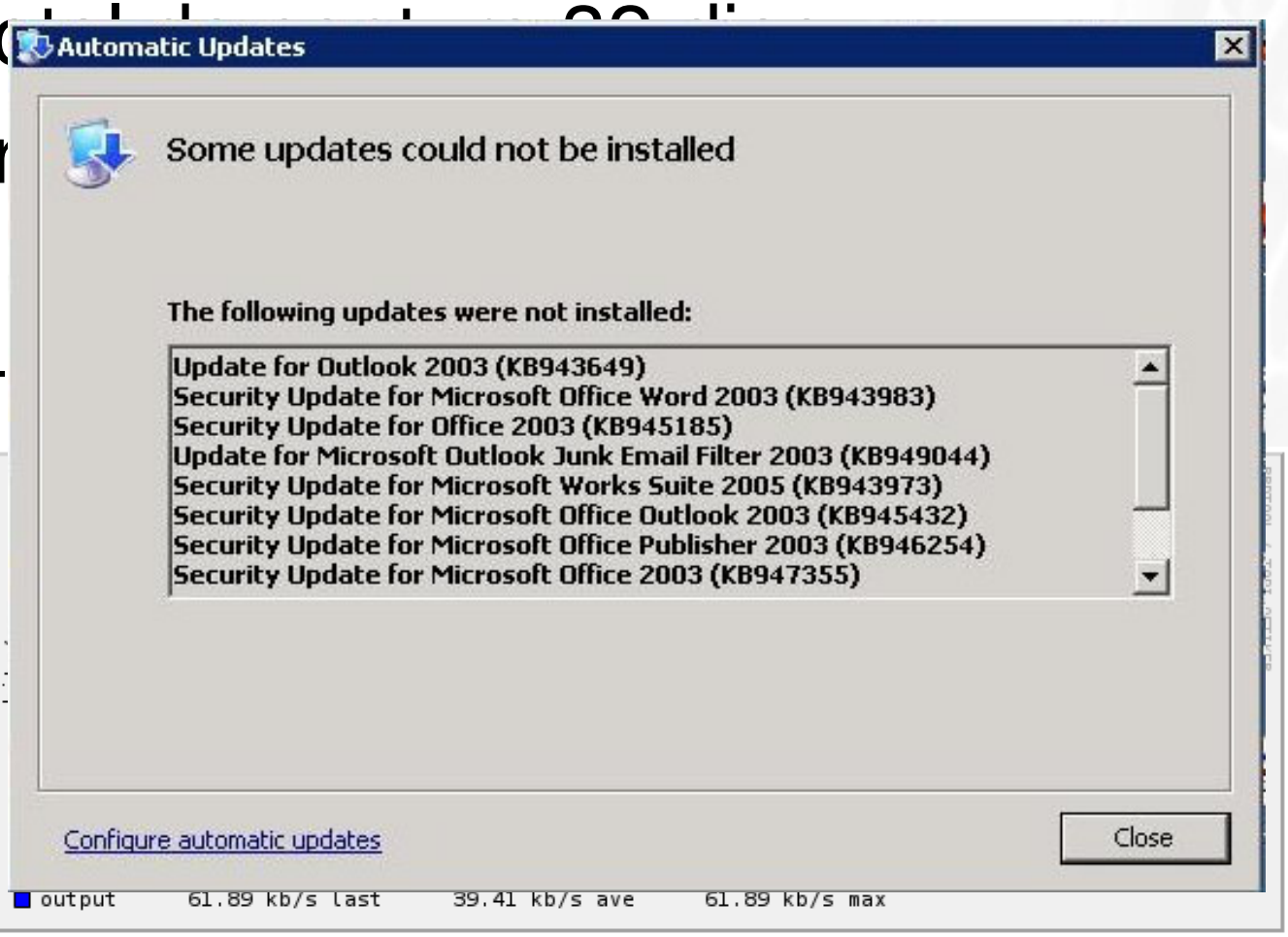
Análise dos resultados

- Total da captura 32 dias
- Tráfego
  - Peculiaridade (1 de maio 2008)



Análise dos resultados

- T
- Tr
  -

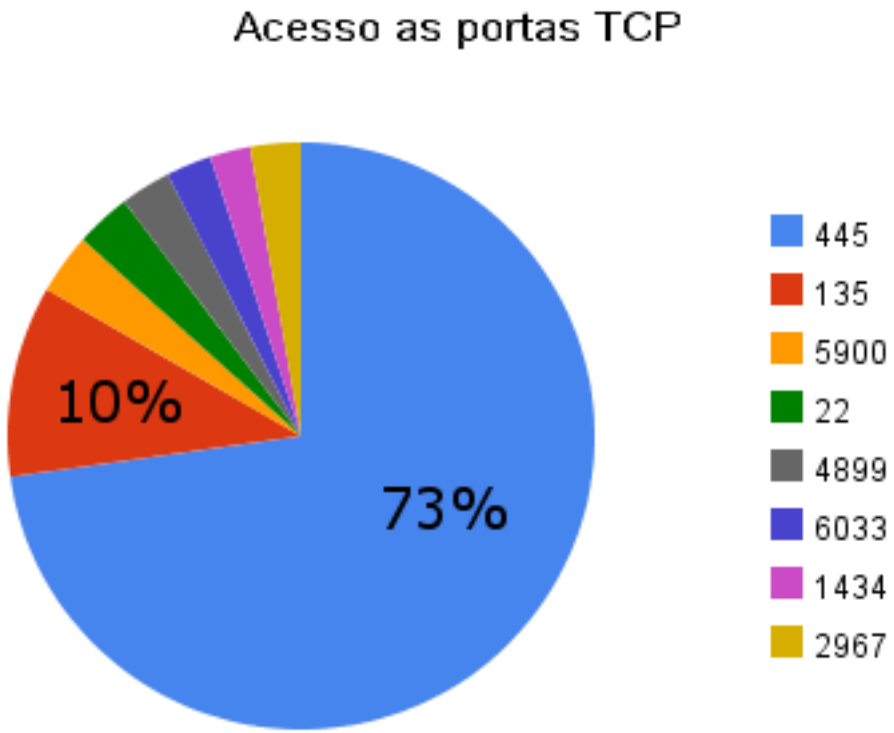


Análise dos resultados

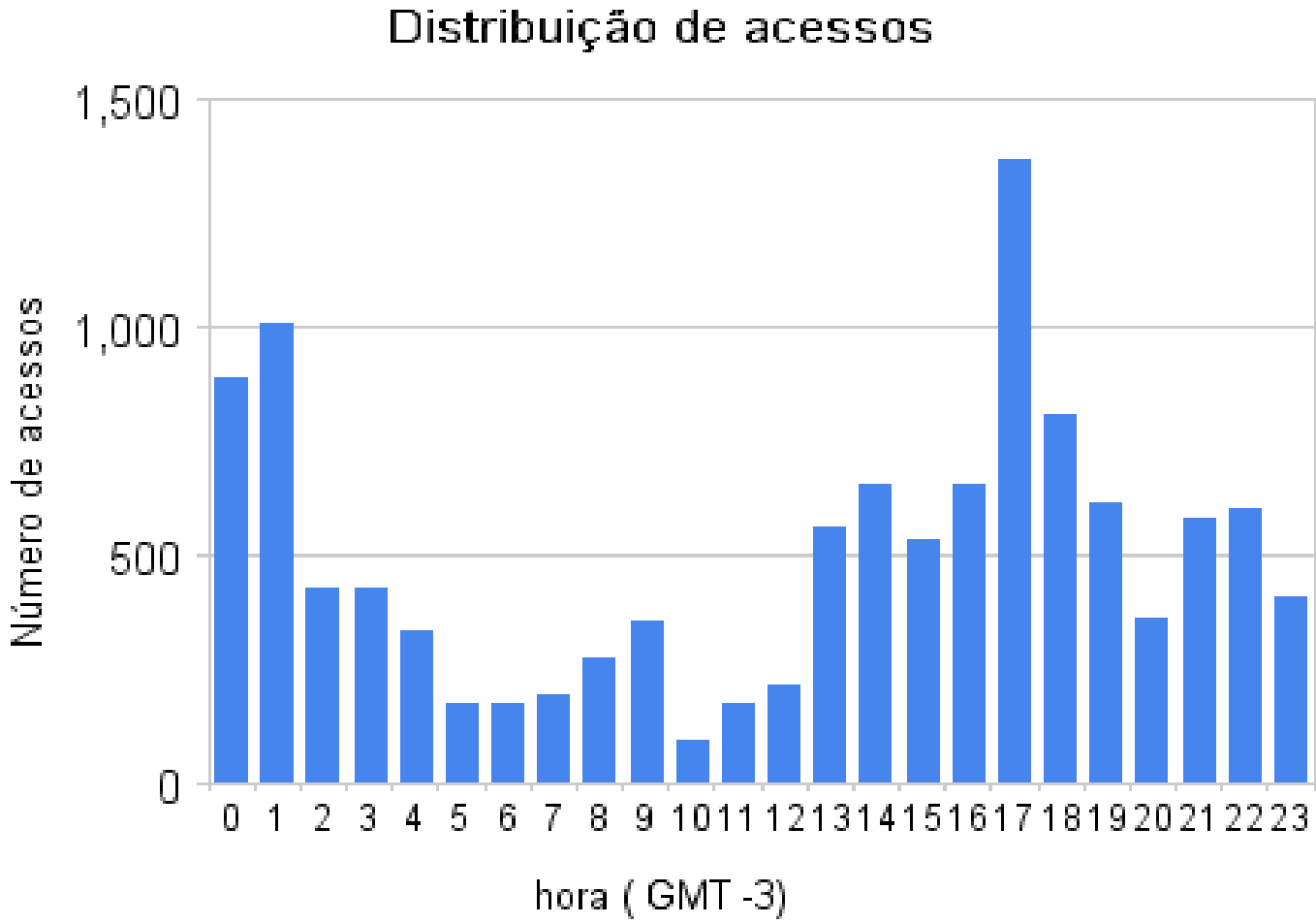
- Análise dos binários
  - Total de acessos: 644.894
  - Total de 26.037 url obtidas de 1.702 IPs distintos
  - Downloads efetivos
    - Download efetivo: 11856
    - Binários únicos: 182

Análise dos resultados

- Portas mais acessadas no honeypot

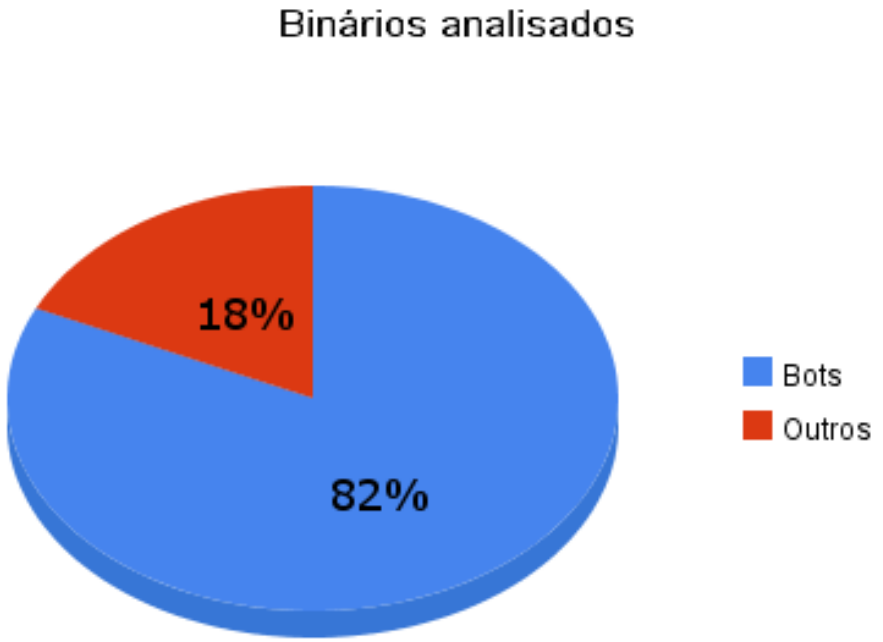


Análise dos resultados



Análise dos resultados

- Total de binários únicos e passiveis de análise



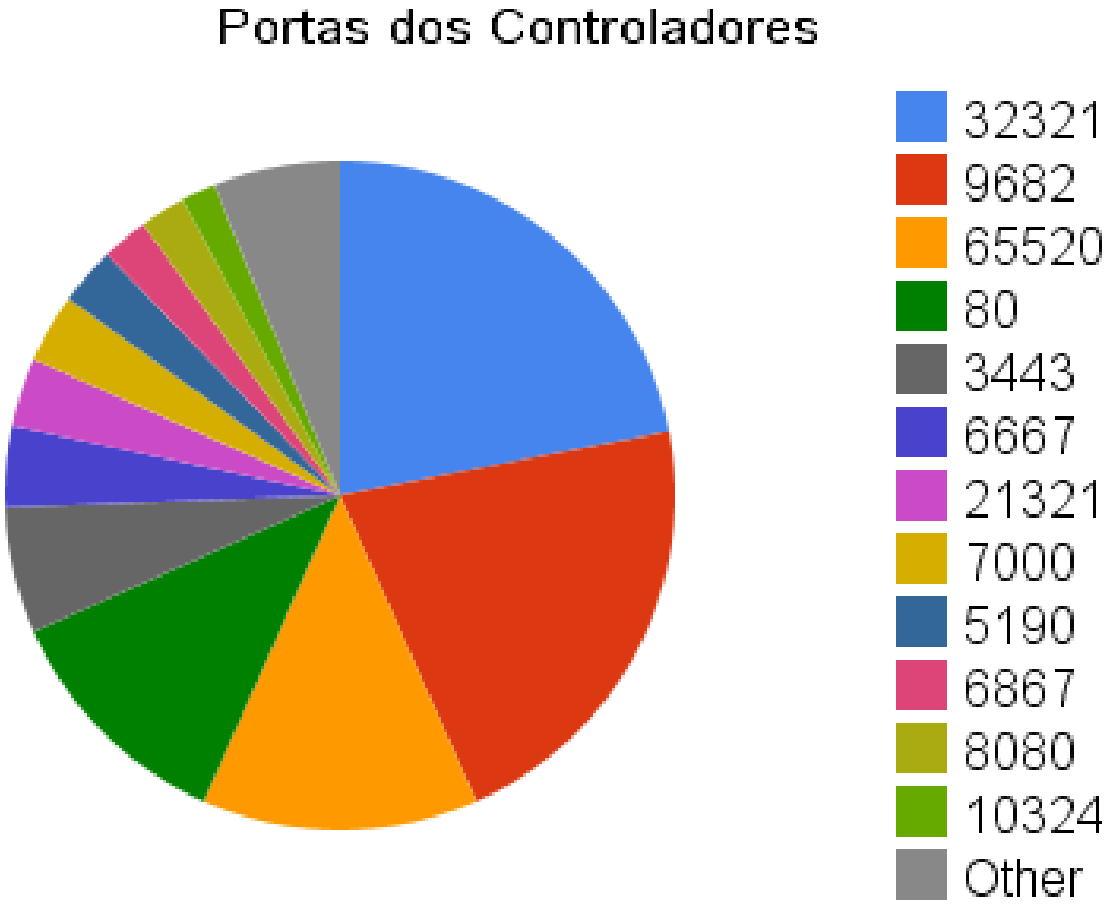
Análise dos resultados

- Controladores de *bots*
  - Total de 34 controladores únicos

51	66.X.X.X
39	85.X.X.X
18	66.X.X.X
15	66.X.X.X
4	67.X.X.X
4	66.X.X.X
3	67.X.X.X
3	211.X.X.X
2	69.X.X.X

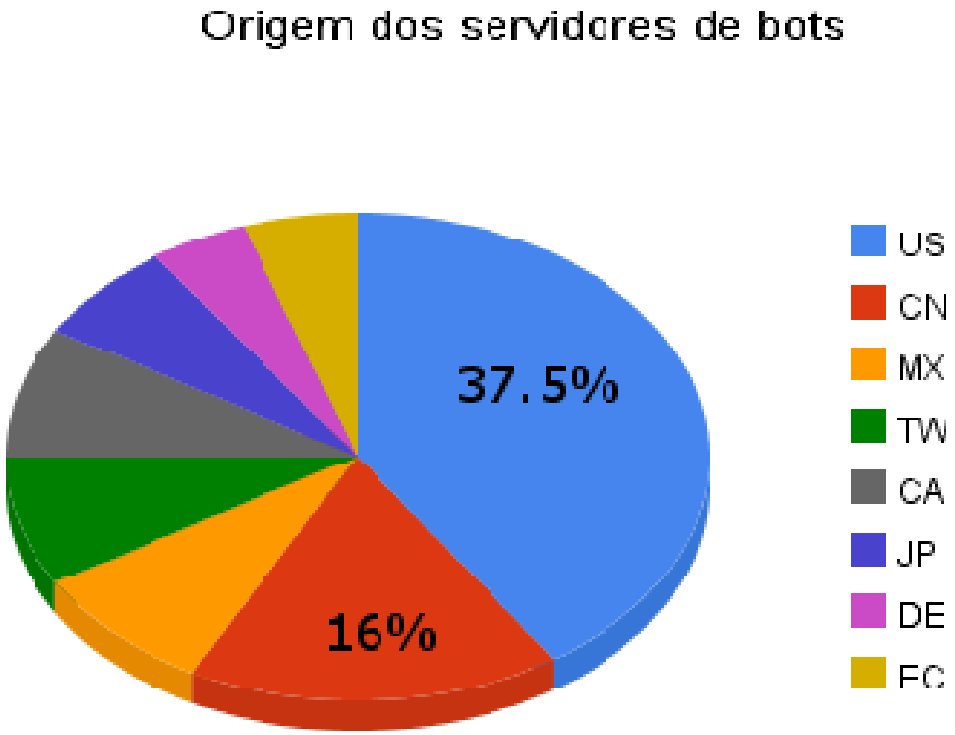
66%

Análise dos resultados



Análise de resultados

- Controladores de *bots*



Análise dos resultados

- Flow filter: src ip 85.X.X.X and dst port 80 (controlador de bots)

Date flow start	Src IP Addr:Port		Dst IP Addr:Port
2008-05-30 13:20:39.775	200.132.X.X:4317	->	85.X.X.X:80
2008-05-30 13:37:49.259	200.160.X.X:1863	->	85.X.X.X:80
2008-05-30 13:58:38.972	200.132.X.X:4317	->	85.X.X.X:80
2008-05-30 14:23:44.068	200.160.X.X:59945	->	85.X.X.X:80
2008-05-30 14:23:43.792	200.160.X.X:1863	->	85.X.X.X:80
2008-05-30 14:33:19.001	200.160.X.X:36310	->	85.X.X.X:80
2008-05-30 15:00:23.580	200.132.X.X:4317	->	85.X.X.X:80
2008-05-30 15:14:29.918	200.160.X.X:36310	->	85.X.X.X:80
2008-05-30 15:27:04.766	200.160.X.X:1863	->	85.X.X.X:80
008-05-30 15:30:24.971	200.160.X.X:59945	->	85.X.X.X:80

Análise dos resultados

- Ferramenta
  - Script que consulta possíveis servidores *bots*
  - Filtrar os IPs sob nossa responsabilidade
  - Gerar notificações automáticas para os responsáveis

Conclusão

- Captura automatizada de binários via *honeynet*
- Análise automática de binários
  - Padrões de rede
  - Controladores de bot
- Análise dos dados em fluxos de rede
- Ferramenta para segurança a nível de *backbone*

Apoio

PoP-RS
Ponto de Presença da
RNP no Rio Grande do Sul

UFRGS
UNIVERSIDADE FEDERAL
DO RIO GRANDE DO SUL

Cert-RS
Computer Emergency Response Team - Rio Grande do Sul

cgi.br
Comitê Gestor da Internet no Brasil

RNP
Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil

Obrigado

Perguntas?

ceron@tche.br