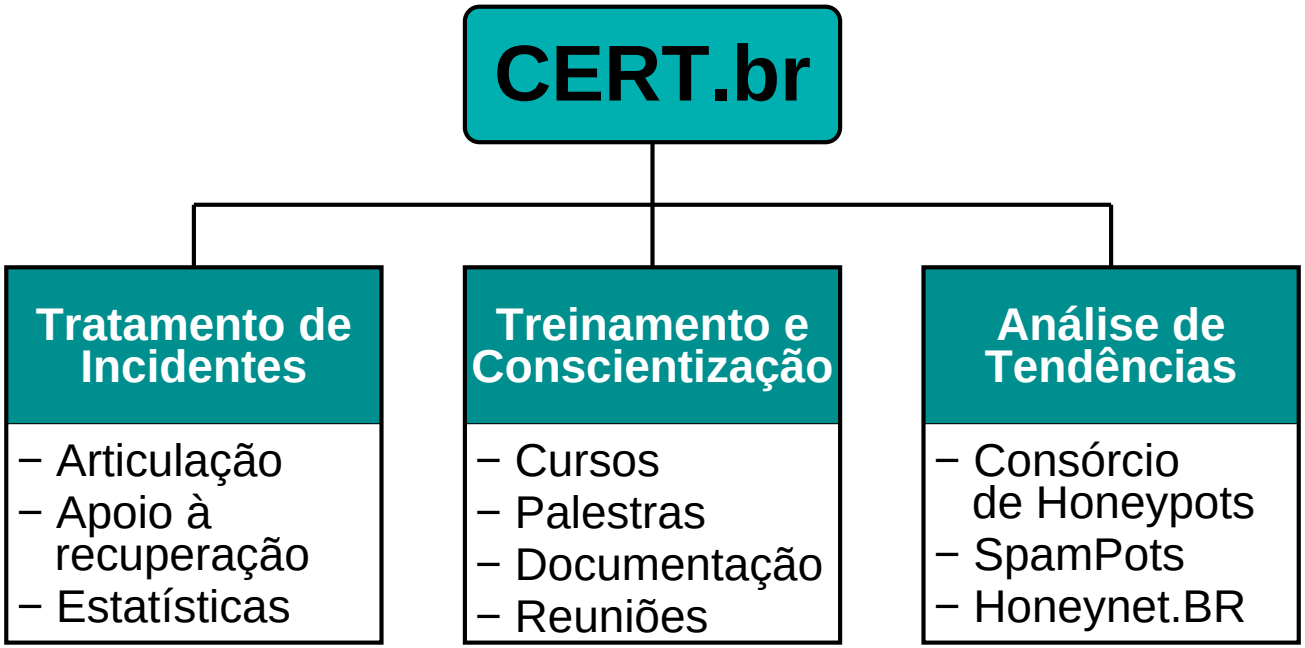
Tendências em Atividades Maliciosas na Internet Brasileira

Klaus Steding-Jessen
jessen@cert.br

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

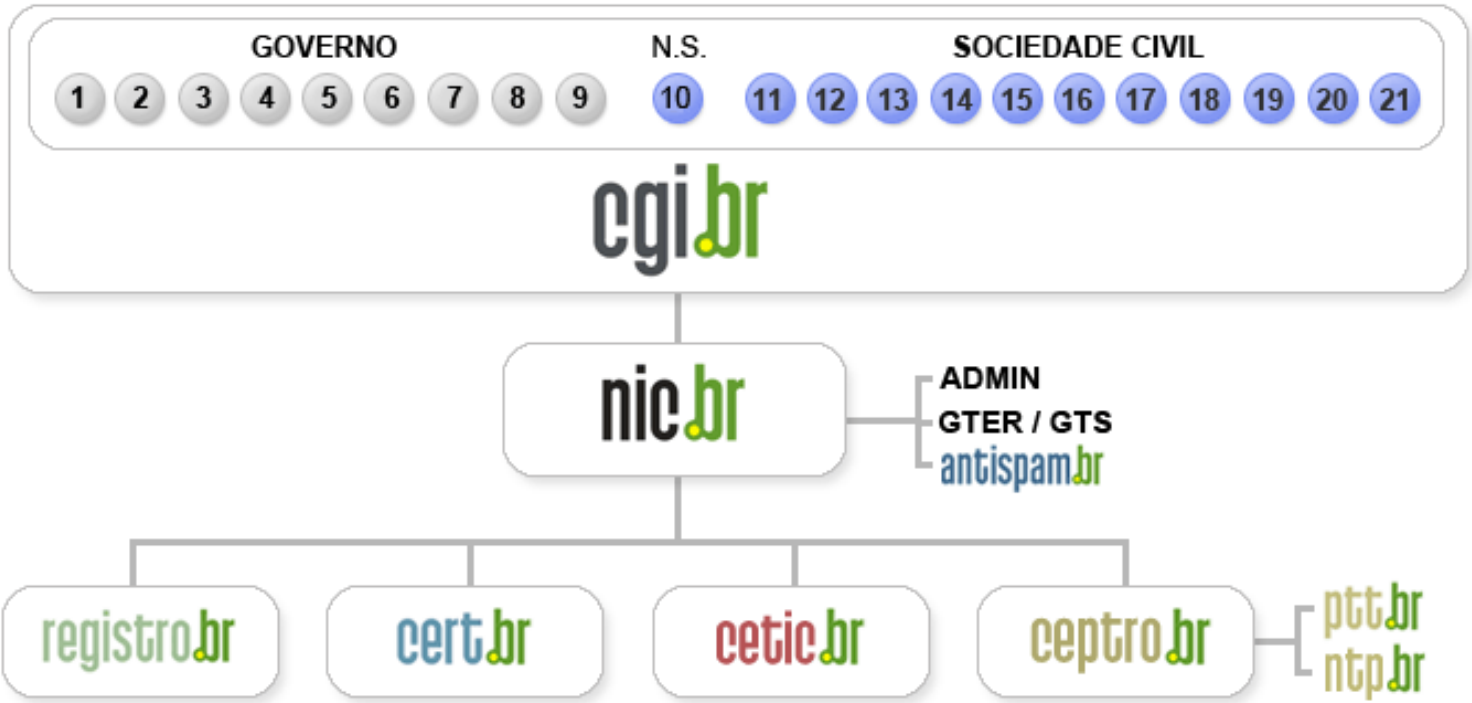
APWG

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

Agenda

- Situação Atual
  - Características dos Ataques
  - Facilitadores para este Cenário
- Incidentes sendo Tratados
  - Tentativas de Fraude
  - Abuso das Redes para Envio de Spam
  - Ataques de Força Bruta
  - DNS
- Considerações Finais
- Referências

Situação Atual

Características dos Ataques

- Amplo uso de ferramentas automatizadas de ataque
- *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
- Usuários finais passaram a ser alvo

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*
- Crime organizado
  - Aliciando *spammers* e invasores
  - Injetando dinheiro na "economia *underground*"

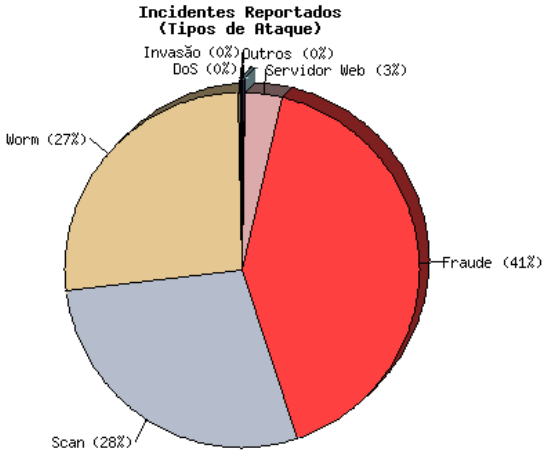
Facilitadores para este Cenário

- Pouco enfoque em Segurança de *Software* e Programação Segura
  - vulnerabilidades freqüentes
  - códigos maliciosos explorando as vulnerabilidades em curto espaço de tempo
- Sistemas e redes com grau crescente de complexidade
- Organizações sem políticas de segurança ou uso aceitável
- Sistemas operacionais e *softwares* desatualizados
  - pouco intuitivos para um usuário
- Falta de treinamento

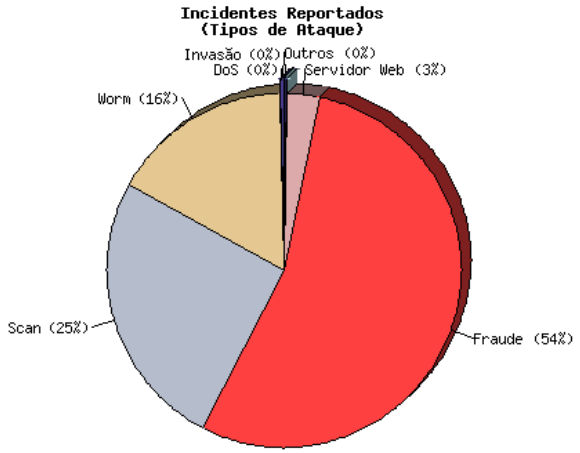
Incidentes sendo Tratados

Tentativas de Fraude

2008 — Jan–Mar



2008 — 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 financeira:

- **Em nome de várias instituições, com tópicos diversos**
- **Com links para cavalos de tróia**
- ***downloads* involuntários, via códigos JavaScript, ActiveX, etc, em máquinas vulneráveis**

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

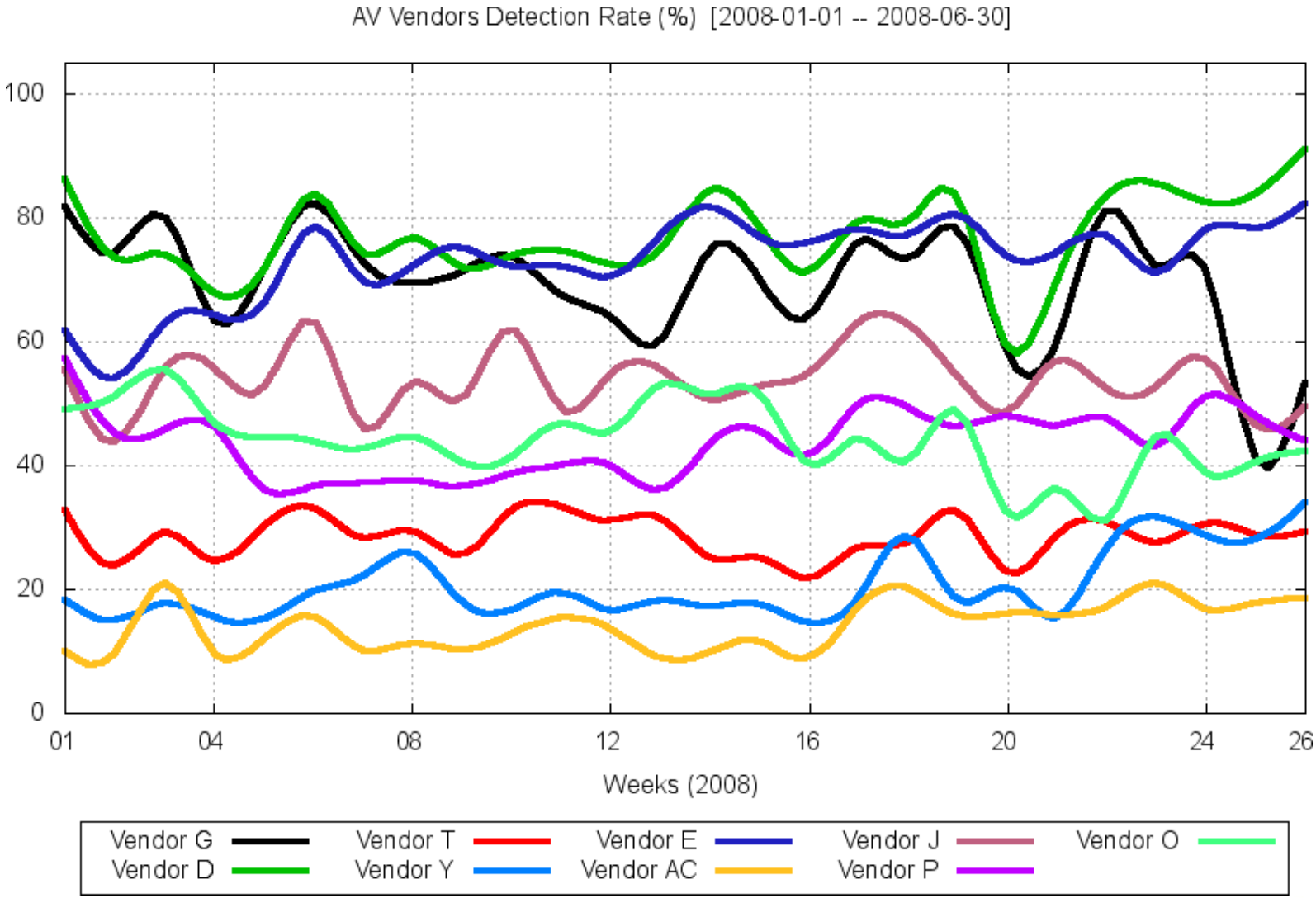
1º Semestre/2008

Detalhes dos Códigos e URLs relacionadas com tentativas de fraude:

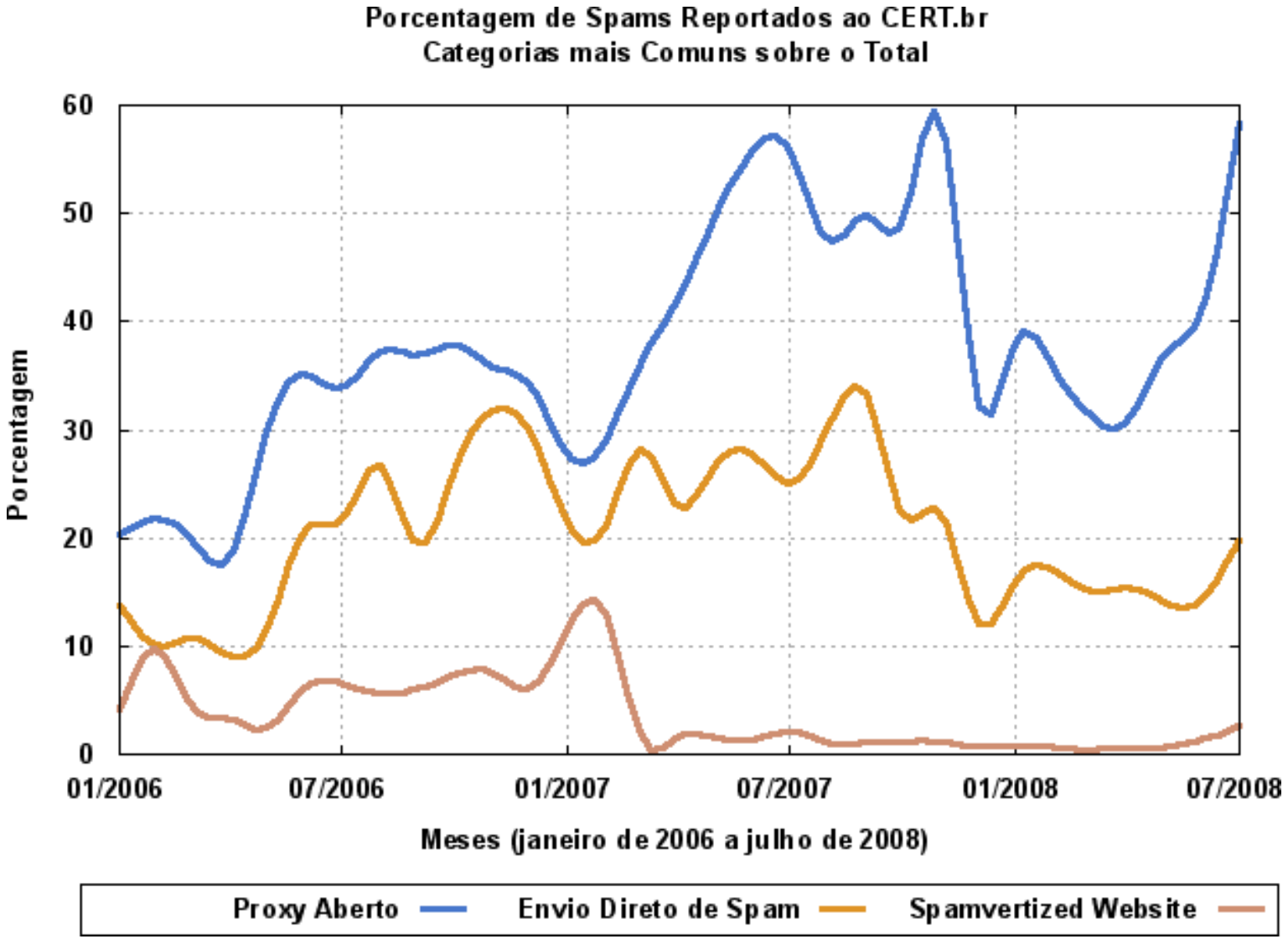
Assinaturas de antivírus (únicas)	3.322
Assinaturas de antivírus (”famílias”)	101
Códigos maliciosos únicos (hashes criptográficos únicos)	8.159
Extensões de arquivos usadas	80
Nomes de arquivos	5.181
URLs únicas	10.022
Domínios	3.708
Endereços IP únicos	2.448
Países de origem	70
URLs notificadas	12.440
Emails de notificação enviados pelo CERT.br	9.104

1º Semestre/2008

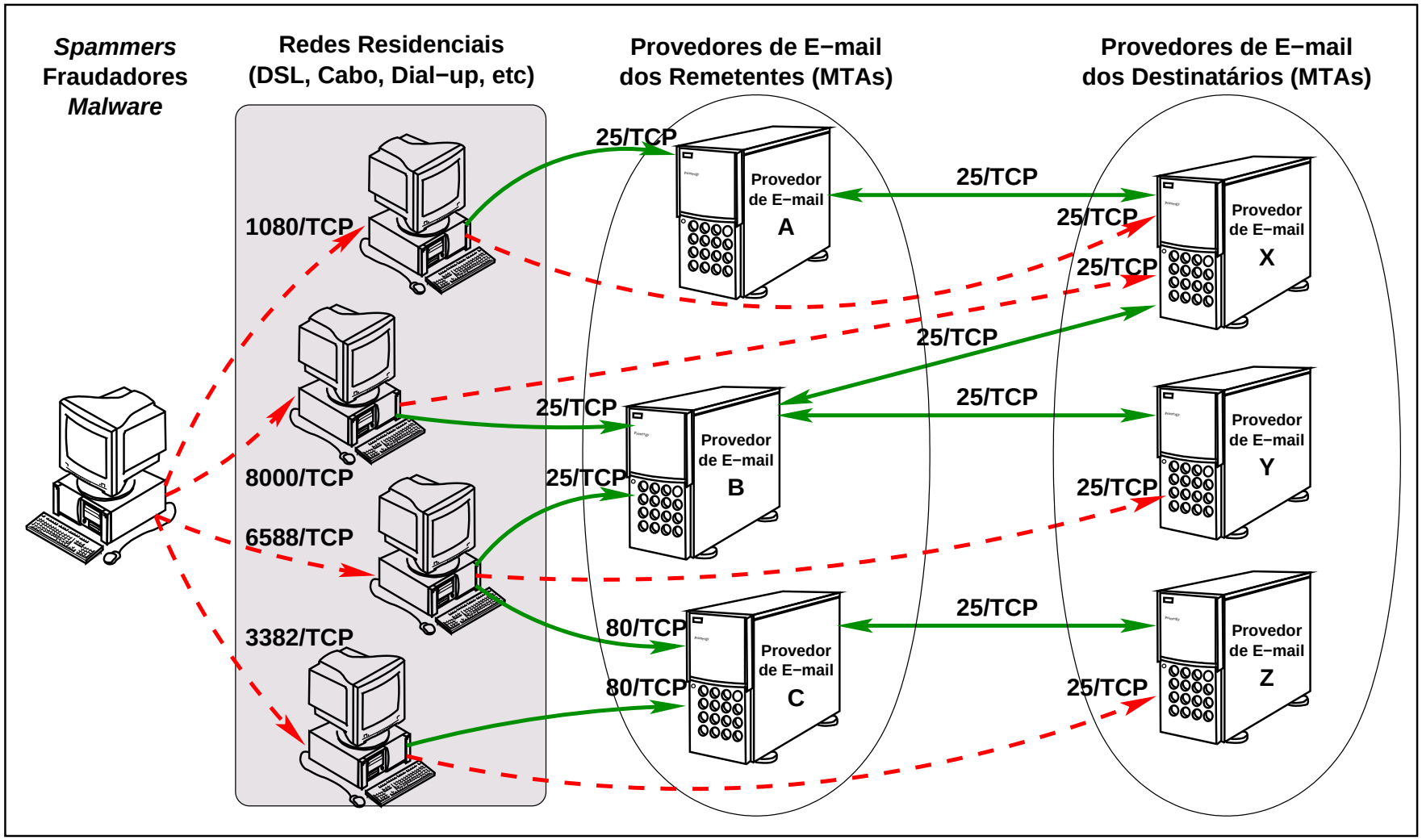
Eficiência dos Antivírus:



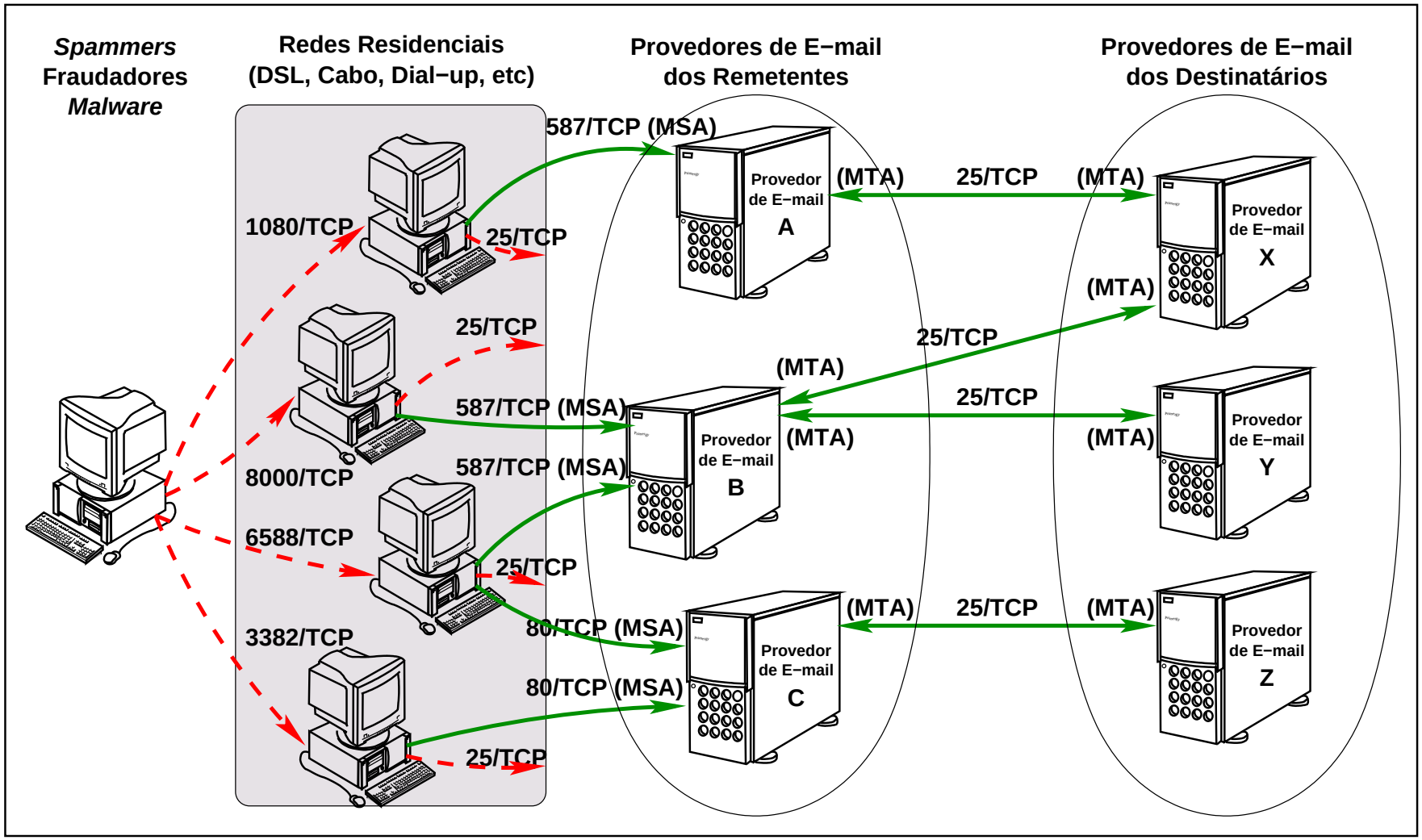
Abuso das Redes para Envio de *Spam*



Como Ocorre esse Abuso



Como Mitigar – Gerência de Porta 25



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/

DNS *Cache Poisoning* (1/2)

- Leva um servidor recursivo a armazenar informações forjadas
  - Permite redirecionamento de domínios para IPs com conteúdo malicioso
- Facilitado pelo método descoberto por Dan Kaminsky
- Correções dos *softwares*: uso de portas de origem aleatórias nas consultas
  - Não elimina o ataque, apenas retarda seu sucesso
  - Adoção de DNSSEC é uma solução mais definitiva

    http://registro.br/info/dnssec.html
- Notificações enviadas pelo CERT.br: $\approx$ 11k

DNS *Cache Poisoning* (2/2)

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

http://www.doxpara.com/DMK_BO2K8.ppt

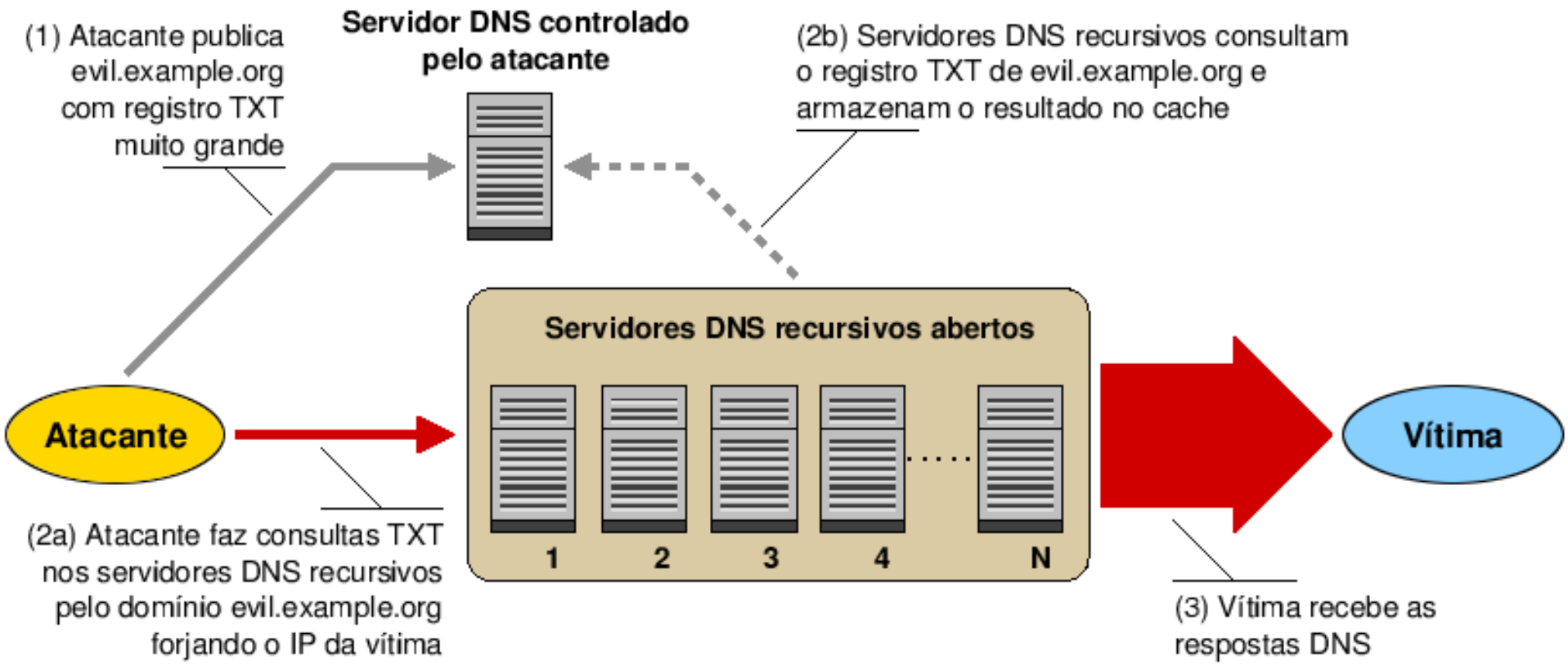
http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNS Recursivo Aberto (1/2)

- Permite que qualquer máquina faça consultas
- É a configuração padrão da maioria dos *softwares* DNS
- Pode ser usado como amplificador em ataques de DDoS
- Recursivos abertos no Brasil:
  - Notificações realizadas pelo CERT.br: $\approx$ 46k
  - Ainda listados pelo *Measurement Factory*: $\approx$ 10k
- Recursivos abertos no mundo:
  - Listados pelo *Measurement Factory*: $\approx$ 338k

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

DNS Recursivo Aberto (2/2)



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

Considerações Finais

Investir em Segurança de *Software*

- Considerar 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/

Proteger a Infra-Estrutura

- Definir Políticas e Procedimentos
- Manter atualizados e aplicar *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
- Implementar práticas de segurança em camadas
  - *firewalls*, IDSs, autenticação, criptografia, etc
- Manter-se atualizado
  - treinamentos, conferências, listas de discussão, *sites* e *blogs* de segurança

Conhecer o Tráfego de sua Rede

- Redes cada vez mais velozes
- Ataques utilizam criptografia
- Necessário ter uma visão geral
- Tecnologias que podem ser usadas para monitoração
  - análise de fluxos de rede (*flows*)
  - *honeypots* de baixa interatividade
- Enfatizar a monitoração do tráfego que sai da sua rede

Referências (1/2)

- Informações sobre *honeypots*
  - *Honeypots* e *Honeynets*: Definições e Aplicações
    http://www.cert.br/docs/whitepapers/honeypots-honeynets/
  - 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
- Ferramentas de código aberto para análise de *flows*
  - https://www.cert.org/netsa/
  - http://www.caida.org/tools/
  - http://qosient.com/argus/

Referências (2/2)

- 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/