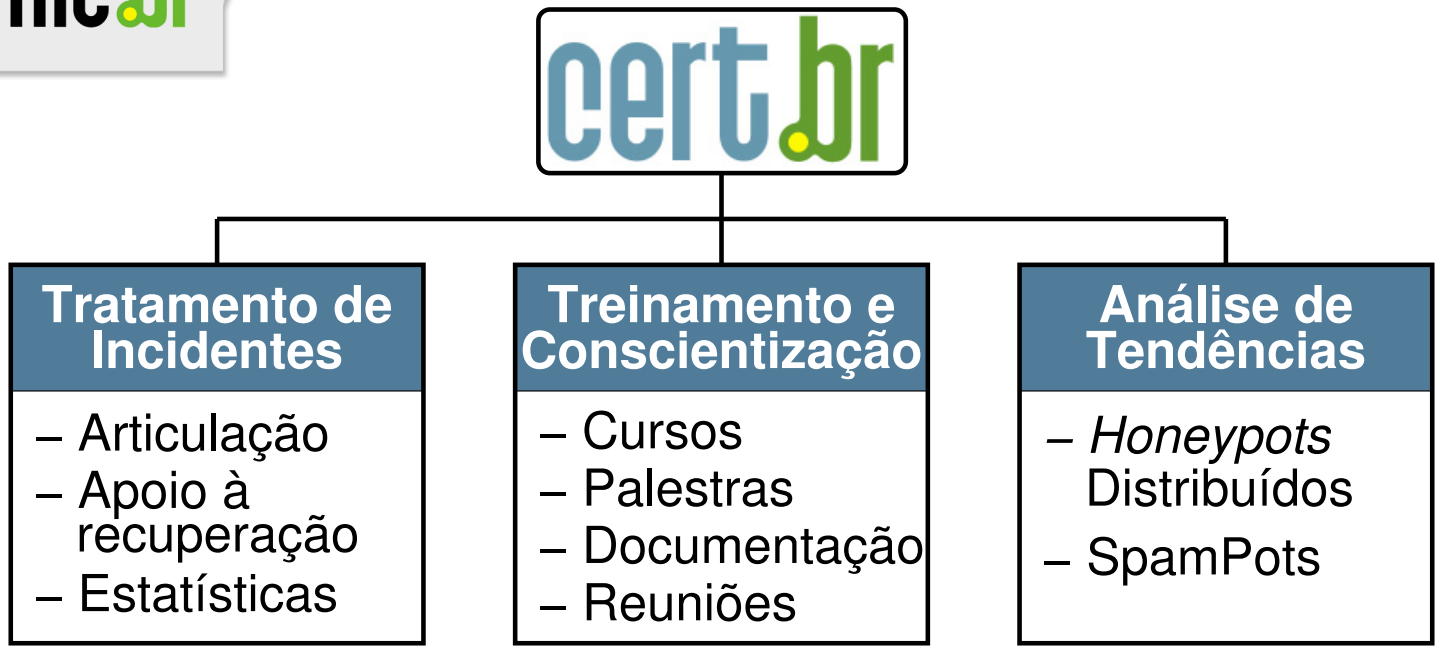
Cartilha de Segurança para Internet e Gerência de Porta 25

Cristine Hoepers
cristine@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

1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. 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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 com os seguintes serviços para o Brasil:

- **ponto de contato nacional para notificação de incidentes**
- **facilitação e o apoio necessários no processo de resposta a incidentes**
- **trabalho colaborativo com outras entidades**
- **conscientização sobre a necessidade de segurança na Internet**
- **auxílio para o estabelecimento de novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança)**

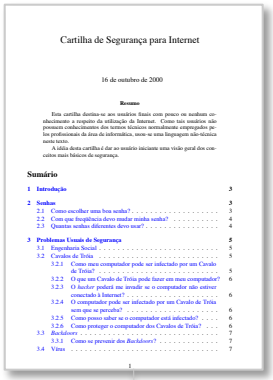
Agenda

- **Cartilha de Segurança para Internet**
  - História
  - Materiais disponíveis
- **Gerência de Porta 25**
  - O problema tratado
  - Como funciona
  - Acordo de cooperação para adoção no Brasil

Cartilha de Segurança para a Internet

Cartilha de Segurança para Internet – Linha do Tempo

1.0


Cartilha de Segurança para Internet

16 de outubro de 2000

Resumo

Esta cartilha destina-se aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet. Como tais usuários não possuem conhecimentos dos termos técnicos normalmente empregados pelos profissionais da área de informática, usou-se uma linguagem não-técnica neste texto.

A idéia desta cartilha é dar ao usuário iniciante uma visão geral dos conceitos mais básicos de segurança.

Sumário

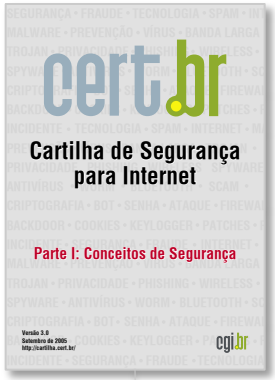
1 Introdução 3

2 Senhas 3
2.1 Como escolher uma boa senha? 3
2.2 Com que freqüência devo mudar minha senha? 4
2.3 Quantas senhas diferentes devo usar? 4

3 Problemas Usuais de Segurança 5
3.1 Engenharia Social 5
3.2 Cavalos de Tróia 5
3.2.1 Como meu computador pode ser infectado por um Cavalo de Tróia? 5
3.2.2 O que um Cavalo de Tróia pode fazer em meu computador? 6
3.2.3 O *hacker* poderá me invadir se o computador não estiver conectado à Internet? 6
3.2.4 O computador pode ser infectado por um Cavalo de Tróia sem que se perceba? 6
3.2.5 Como posso saber se o computador está infectado? 6
3.2.6 Como proteger o computador dos Cavalos de Tróia? 6
3.3 *Backdoors* 7
3.3.1 Como se prevenir dos *Backdoors*? 7
3.4 Vírus 7

- 20 páginas
- conceitos básicos
- dúvidas frequentes

3.0



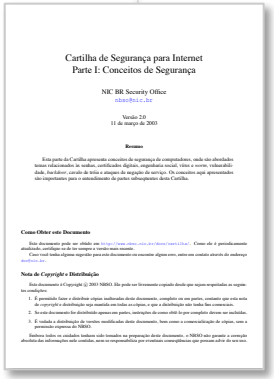
- incluída parte sobre códigos maliciosos
- folder de dicas

4.0

- ilustrada
- eBook (ePub)
- novos temas: redes sociais e dispositivos móveis

2000 2003 2005 2006 2012

- organizada em partes
- incluído o tema de fraudes na Internet


Cartilha de Segurança para Internet
Parte I: Conceitos de Segurança

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, certificados digitais, engenharia social, vírus e worm, vulnerabilidade, *backdoor*, cavalo de tróia e ataques de negação de serviço. Os conceitos aqui apresentados são importantes para o entendimento de partes subsequentes desta Cartilha.

Como Obter este Documento

Nota de *Copyright* e Distribuição

2.0

3.1

- lançada como livro

- fascículos e *slides*

Cartilha de Segurança para Internet 4.0

2ª Edição do Livro

Novas recomendações, em especial sobre

- segurança e privacidade em redes sociais
- segurança no uso de dispositivos móveis

Reestruturada

- ilustrada
- em HTML5
- formato para *tablets*, *smartphones* e *e-readers* (ePub)

Nova licença

- *Creative Commons* (CC BY-NC-ND 3.0)

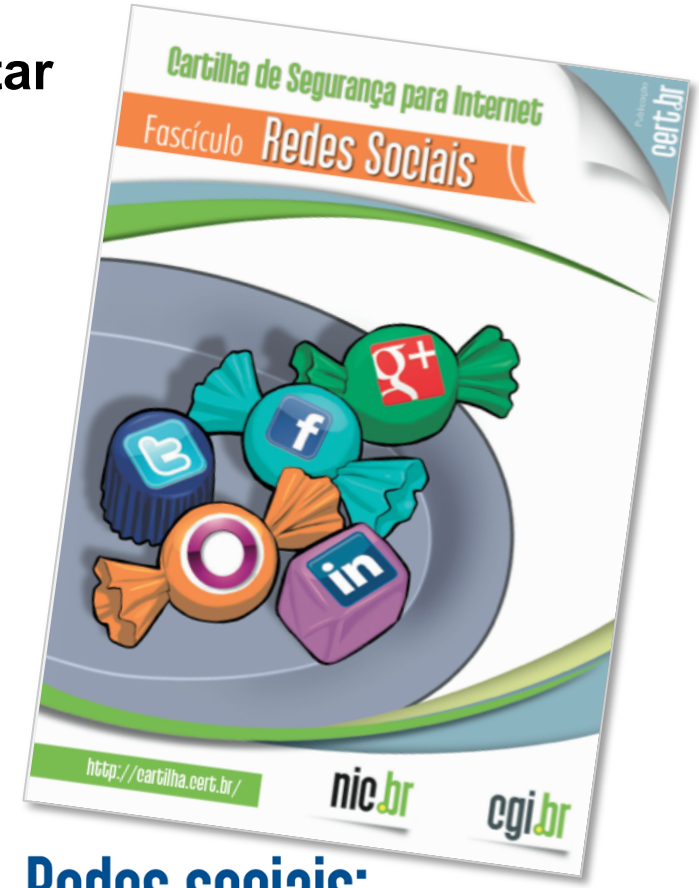
Cartilha de Segurança para Internet – Fascículos

Organizados e diagramados de forma a facilitar a difusão de conteúdos específicos

- **Primeiro Fascículo: Redes Sociais**

***Slides* de uso livre para:**

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**
- **licença CC BY-NC-SA 3.0 Brasil**



Cartilha de Segurança para Internet – Dica do Dia

RSS

http://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Site

http://cartilha.cert.br/

Gerência de Porta 25 no Combate ao Abuso das Redes Brasileiras por *Spammers*

Adoção no Brasil liderada pela Comissão de Trabalho *Antispam* do CGI.br com coordenação técnica do CERT.br

O Problema do Abuso da Infraestrutura de Redes do Brasil por *Spammers* Internacionais

Para ganhar anonimato *spammers* e fraudadores:

- **infectam computadores de usuários finais**
- **subvertem o caminho normal para o envio de *e-mails***

Estudo do CGI.br mostrou que:

- **Mais de 90% do tráfego observado era de tentativas de conectar diretamente em um servidor de *e-mails* do destinatário do *spam***
- **Os *spammers* internacionais abusam as redes do Brasil**
  - **Cerca de 99,9% de todo *spam* que tentou passar pelos sensores vinha de fora do Brasil**
  - **Mais de 90% tinham como destino redes fora do país**

Fonte:

- **Projeto mantido pelo CGI.br/NIC.br, como parte da CT-Spam**
- **Com sensores em 5 operadoras diferentes de cabo e DSL**
  http://www.cert.br/docs/whitepapers/spampots/

Impactos Negativos do Cenário Atual

- **Blocos de IPs das redes brasileiras entram em listas de bloqueio**
  - **servidores de *e-mail* nesses blocos de endereçamento não conseguem enviar *e-mails***
- **A infraestrutura da Internet banda larga do Brasil está sendo utilizada para atividades ilícitas (fraudes, furto de dados, etc)**
- **A banda está sendo consumida por *spammers***
  - **para cada *spam* consome-se 2 vezes a banda internacional, para entrada no Brasil e volta ao exterior**
- **Aumento dos custos operacionais**
  - **mais equipamentos, pessoal e banda para lidar com os *spams***
- **O Brasil é apontado como uma das maiores fontes de *spam* no mundo**

A Gerência de Porta 25

A "Gerência de Porta 25" é uma técnica que:

- **Aplica-se somente a redes de perfil residencial**
  - **IPs dinâmicos**
  - **Dial-up, ADSLs, Cabo e 3G em suas modalidades domésticas**
- **Permitirá diferenciar:**
  - **a submissão de *e-mails* de um usuário para seu(s) provedor(es)**
  - **da transmissão de mensagens entre servidores de serviços de *e-mail***

Implementação da Gerência de Porta 25

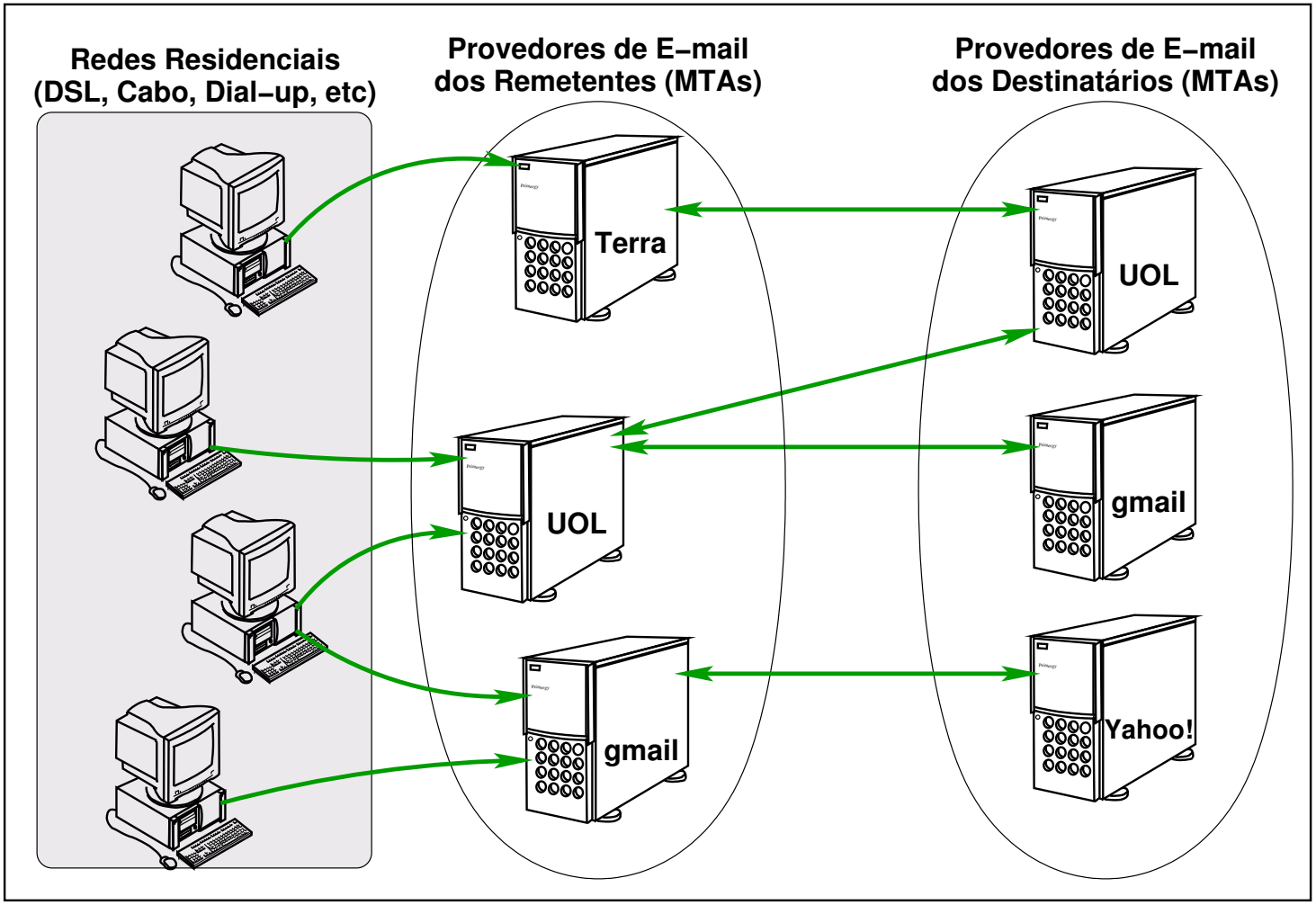
Depende da aplicação de medidas por provedores de *e-mail* e prestadoras de serviços de conectividade:

- **Provedores de *e-mail*:**
  - **Passam a oferecer serviço de submissão de *e-mails* em uma "porta" diferente (a 587 ou a 465)**
  - **Instruem os usuários sobre como configurar seus programas de e-mail (como Outlook, Thunderbird, etc)**
  - **Usuários de *webmail* não precisam fazer mudanças**

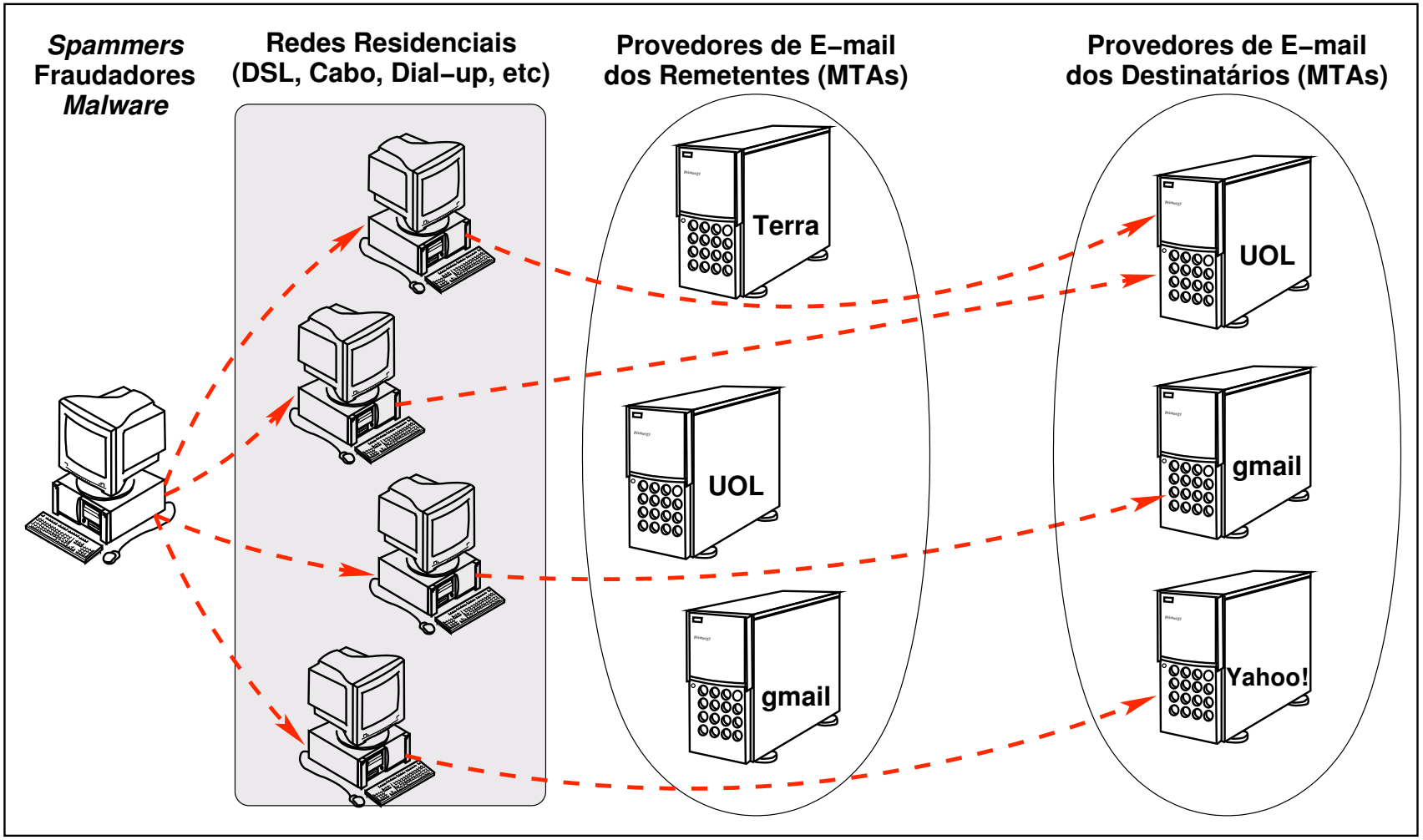
- **Prestadoras de serviços de conectividade residencial:**
  - **Devem filtrar o tráfego de saída com destino à porta 25**
  - **Esse filtro se aplicará apenas a tráfego com origem nessas redes de perfil residencial**

Detalhes em: http://antispam.br/admin/porta25/

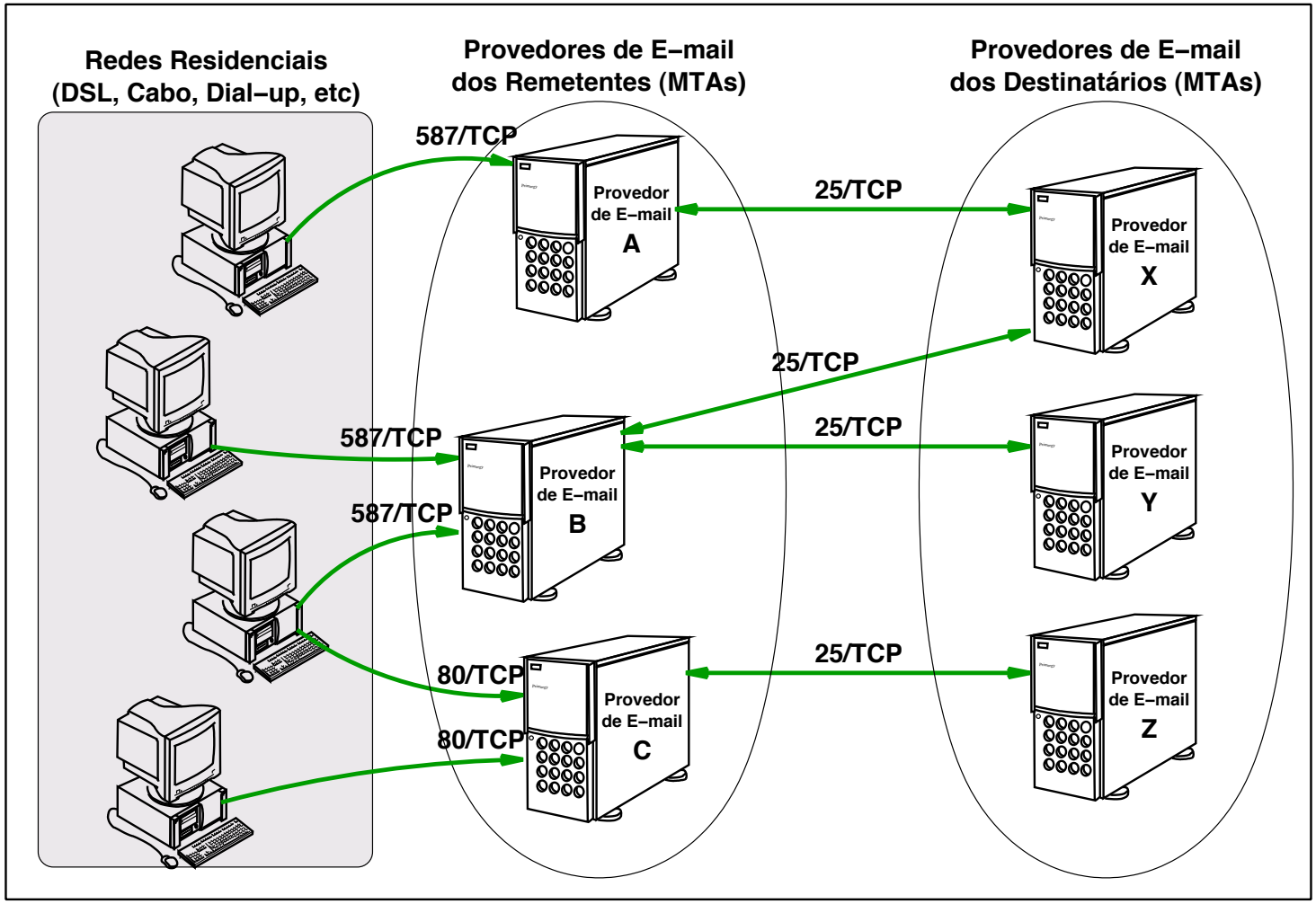
Envio Legítimo de E-mails Hoje



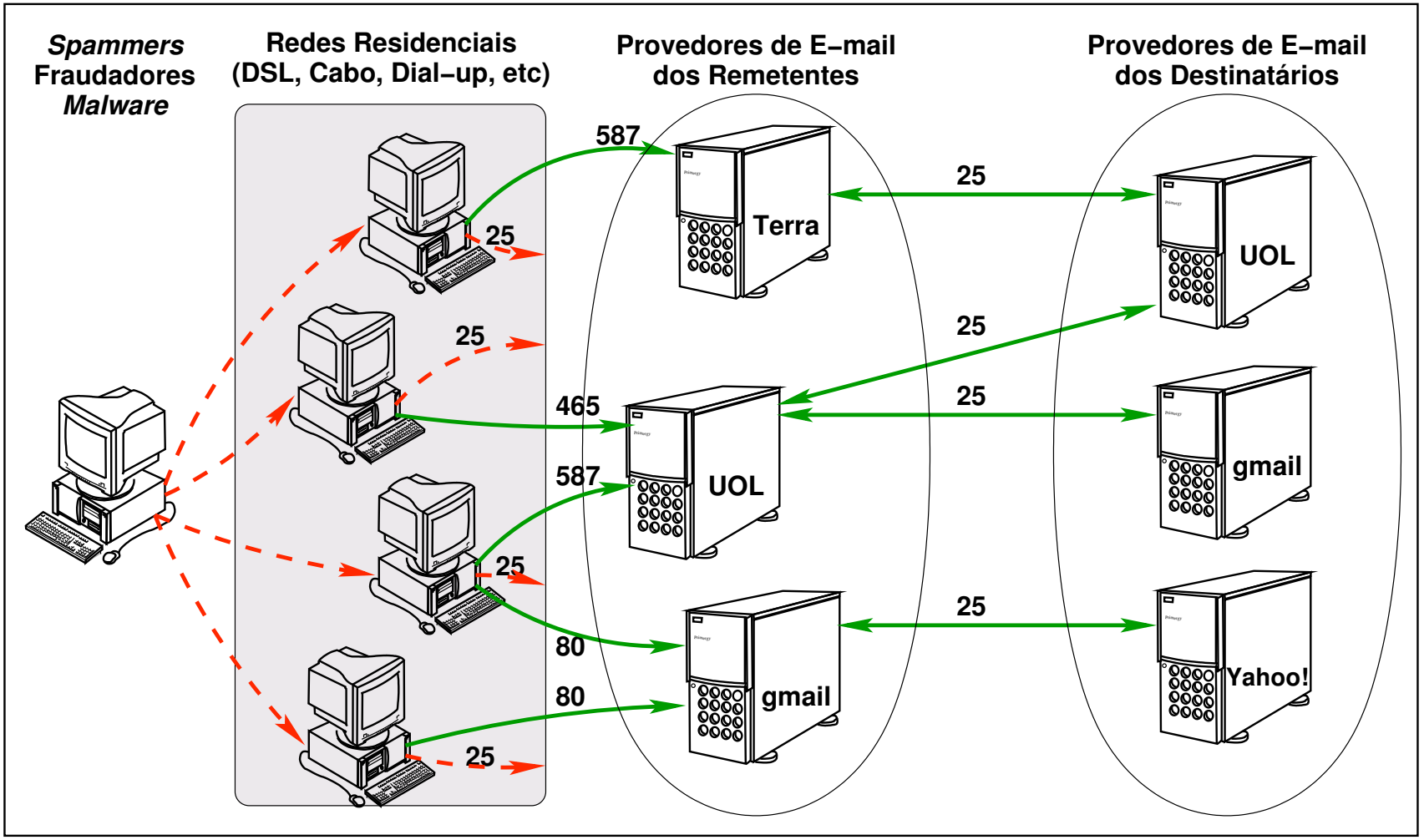
Envio de Spam via PCs Infectados



Uso Legítimo Após a Implantação da Recomendação



Como a Recomendação Impede o Envio Direto



Benefícios da Adoção da Recomendação

- Saída das redes brasileiras de listas de bloqueio de IPs envolvidos no envio de *spam*
- Dificulta o abuso da infraestrutura da Internet para atividades ilícitas (como fraudes, furto de dados, etc).
- Redução do abuso das máquinas dos usuários
  - diminuição na carga dos recursos computacionais
  - redução do consumo de banda para envio de *spam*, com conseqüente melhora nas condições de utilização da rede
- Atua antes do *spam* entrar na infra-estrutura de *e-mail*
  - menos desperdício de banda e menos esforço de configuração de filtros anti-*spam*.
  - diminuição do consumo de banda internacional por *spammers*
  - diminuição de custos operacionais
- Melhora da imagem do Brasil no exterior

Acordo de Cooperação para Implementar a Recomendação da Gerência de Porta 25

Histórico

- Recomendação do CGI para Gerenciamento da Porta 25 em 2009
- 14 reuniões de trabalho com as partes envolvidas de 2008 a 2011
- Elaboração do texto do acordo em Julho de 2010
- Aprovação do acordo pela Anatel em Abril de 2011
- Endosso do acordo pelo Ministério da Justiça (DPDC) em Outubro de 2011
- Assinatura do acordo em 11 de Novembro de 2011
- Implementação durante o ano de 2012

Andamento

- **Associações de provedores / prestadores de serviço de correio eletrônico**
  - **Acompanharam a adesão de seus associados ao acordo**

- **Prestadoras de serviço de conectividade**
  - **Em fase final de planejamento do bloqueio da saída de tráfego com destino à porta 25**
    - **para usuários de redes domésticas com IP dinâmico**

Cristine Hoepers
cristine@cert.br

- CGI.br - http://cgi.br/
- NIC.br - http://nic.br/
- CERT.br - http://cert.br/

  ✓ Cartilha de Segurança para Internet
  http://cartilha.cert.br/

  ✓ Gerência de Porta 25
  http://antispam.br/admin/porta25/