Spam: eles venceram?

Danton Nunes, InterNexo Ltda.
danton.nunes@inexo.com.br

Novas técnicas de spam

Abuso de formulários na Web

Consiste em abusar formulários tipo "fale conosco" para enviar e–mail. Equivalente a open–relay.
Derrota SPF e Greylisting

Spambots "inteligentes"

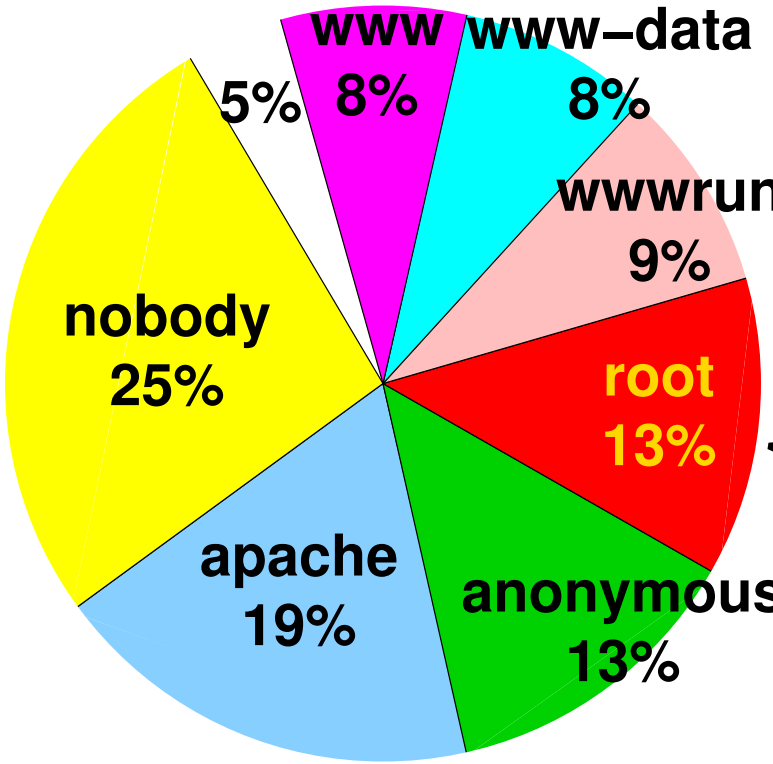
Spambots que simulam MTAs válidos, reconhecendo erros transitórios e com fila para envio.
Derrota Greylisting

Mensagens embutidas em imagens

Imagens contendo textos. Inicialmente mensagens com uma só imagem, atualmente mosaicos complexos
Desafia filtros de conteúdo

Abuso de formulários na Web

Estatísticas em 1112 mensagens recebidas
Divisão por nome de usuário do servidor Web



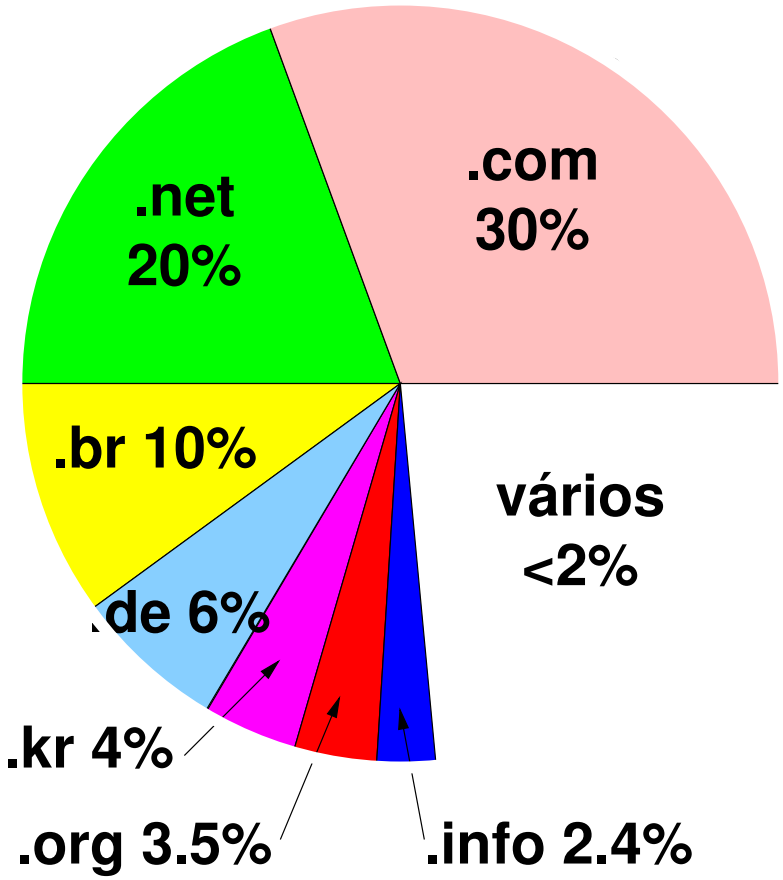
É possível filtrar pelo envelope com algum sucesso

isto é muito preocupante!

Danton Nunes, InterNexo Ltda.

Abuso de formulários na Web

Estatísticas em 1112 mensagens recebidas
Divisão por nome de domínio (só TLDs)



Origens de spams por formulários na Web são bem espalhadas pelos TLDs.

Portanto não é uma boa idéia bloquear pelo nome de domínio no envelope.

Danton Nunes, InterNexo Ltda.

Abuso de formulários na Web

Técnicas de combate:

- **SPF**

  falha, pois a mensagem vem de transmissor válido.

- **Greylisting**

  falha, pelo mesmo motivo.

- **Lista negra**

  falha pois raramente transmissores válidos estão listados.

- **Envelope**

  sucesso relativo em bloquear este tipo de spam mas há riscos de falsos positivos.

Spambots "inteligentes"

Spambot clássico

Não tenta enviar novamente quando recebe erro temporário (princípio de funcionamento da greylist)

"Entregam" o endereço IP da origem

Novos spambots

Mantém o estado dos destinatários e reenvia em caso de erro temporário (greylist killer)

Disfarçam o endereço de origem inserindo cabeçalhos falsos.

Spambots "inteligentes"

Técnicas de combate:

- **SPF**

  funciona, mas os spammers preferem domínios sem SPF.

- **Greylisting**

  falha, pois o spambot não desiste após receber erro 4xx

- **Lista negra**

  funciona, spambots rodam normalmente em dialups, mas as listas negras em si trazem muita dor de cabeça.

- **Envelope**

  falha. os envelopes são mais falsos que nota de sete.

Mensagens embutidas em imagens

Primeira geração (final de 2005)

Imagem única embutida em HTML.

Padrão facilmente reconhecível, logo os filtros de conteúdo aprenderam a identificar essas mensagens.

Segunda geracão (aprox. abril de 2006)

imagens múltiplas em mosaico, com suporte em HTML.

Alta variabilidade quanto ao número e disposição das imagens => menos detectável por filtto de conteúdo.

Mensagens embutidas em imagens

Normalmente enviadas por spambots "espertos" para driblar greylisting.

A mensagem aberta na tela de um agente de usuário que suporta HTML se parece com um texto simples, com pouca decoração.

Ainda não vi uma mensagem dessas com cavalos de Tróia ou vírus, mas a ausência de evidência não é uma evidência da ausência, porisso, olho vivo!

HTML em e–mail bem que podia ser desinventado!

Conclusões

As novas técnicas de envio de spam certamente surgiram em resposta ao uso crescente de SPF e greylisting.

O relativo sucesso delas mostra o que já sabiamos há muito tempo, que o combate ao spam tem que ser feito na origem. Administradores de redes corporativas e de ISPs, no entanto, tem se mostrado negligentes e evitam entrar em atrito com seus clientes (p.ex. fechar a porta 25/tcp cria celeuma)

Visite http://www.antispam.br/