



Técnicas de redução de spam

Rubens Kühl Jr.
LARC/USP & Ética Tecnologia
rubens@email.com



Cenário

- Volume rapidamente crescente
- Spam como negócio
- Comportamento "stealth"
 - Identificação fraudulenta, variação de conteúdo, open-relays, open-proxies, IP hijacking
- Farto uso de máquinas comprometidas (inclusive através de worms)
- Isolamento crescente do Brasil
- Falta de consenso entre os prejudicados



Medidas de defesa

- Bloqueio x tagging
- DNS Blacklists
- Filtros de conteúdo
- Desafio-resposta
- Greylisting
- Verificação de credibilidade



DNS Blacklists

- Spam-sources
 - bl.spamcop.net
- Open-relays
 - <http://www.ordb.org>
- Open-proxies
- Dial-up/IPs dinâmicos
 - dialups.services.net
- Credibilidade
 - <http://www.isipp.com/iadb.php>



Filtros de conteúdo

- Conteúdo estático (“Buy Viagra Now”)
- Conteúdo dinâmico
 - <http://www.rhyolite.com/anti-spam/dcc/>
- Estatística de Bayes
- Anti-vírus
- Táticas evasivas
- Ferramentas
 - <http://www.spamassassin.org>
 - <http://www.mailscanner.info>



Desafio-resposta

- Verifica “humanidade” do emissor
- Impõe carga de envio de desafio, processamento da resposta
- Depende de configuração do usuário para e-mails automáticos
- Tipicamente controverso
- Implementações free disponíveis
 - <http://www.tmda.net>,
 - <http://www.paganini.net/ask>



Greylisting

- Spammers não retentam entregas SMTP (exceto em caso de open-relay)
- São gerados erros temporários em função do padrão de e-mail (IP ou combinação IP + remetente + destinatário)
- Implementação por software específico
 - <http://projects.puremagic.com/greylisting/>
- Implementação por infra-estrutura
 - Sistema “funcionário-público” ou “fila-de-banco”



Verificação de credibilidade

- Este e-mail é de fonte garantida opt-in ?
 - Habeas (<http://www.habeas.com>)
 - Bonded Sender (<http://www.bondedsender.com>)
 - IADB (<http://www.isipp.com>)
- Este e-mail é da onde diz ser ?
 - Pesquisas da IRTF/ASRG (<http://asrg.sp.am>)
 - Por IP: SPF (<http://spf.pobox.com>), MS Caller-ID (http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.msp)
 - Por autenticação: Yahoo! DomainKeys, outras propostas em estudo no ASRG



Medidas de contenção

- Não basta bloquear, tem que participar
- SMTP AUTH
- Filtragem de SMTP/OpenProxy
- Transparent proxy de SMTP(outbound)
- Mail submission port (tcp/587)
- Limitação de taxas
 - Vazão de E-mails, vazão de destinatários
 - Destinatários únicos por intervalo de 15 min



Referências e Perguntas

- DNSBL de spams em progresso SpamCop - <http://www.spamcop.net>
- DNSBL de open-relays ORDB - <http://www.ordb.org>
- DNSBL dialups.services.net da SpamBR - <http://spambr.org>
- DNSBL + serviço de credibilidade IADB - <http://www.isipp.com/iadb.php>
- Assinaturas de spams - <http://www.rhyolite.com/anti-spam/dcc/>
- Desafio-resposta - <http://www.tmda.net>, <http://www.paganini.net/ask>
- Greylisting - <http://projects.puremagic.com/greylisting>
- Software Spam Assassin - <http://www.spamassassin.org>
- Software Mail Scanner - <http://www.mailscanner.info>
- Serviço de credibilidade Habeas - <http://www.habeas.com>
- Serviço de credibilidade Bonded Sender - <http://www.bondedsender.com>
- ASRG(Anti-spam Research Group) - <http://asrg.sp.am>
- Credibilidade de origem método SPF - <http://spf.pobox.com>
- Credibilidade de origem método Microsoft Caller-ID - http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx
- NIC BR Security Office (NBSO) – <http://www.nbso.nic.br>