A praga do *spam*

Bruno Castro*

(continuação do n.º 174)

Categorias e Técnicas de spam

As organizações que utilizam e promovem o conceito de *spam* necessitam de organizar, de forma sistematizada, os *alvos* a atacar massivamente a Internet. Essa organização de *alvos* baseia-se na construção e manutenção de listas dinâmicas de endereços de correio electrónico, denominadas de ***alvos***. Existem várias formas de o fazer, nomeadamente na utilização de aplicações automatizadas de angariação de endereços de correio electrónico, ou sincronização de listas de *spam* adicionais, ou através de pesquisas automatizadas de sites web com referências a servidores de correio electrónico dentro do código HTML (*tags* "mailto:"). Outra forma de angariar *alvos*, ou de dinamizar as várias listas de *spam* existentes na Internet, é através de compra e venda de listas de endereços de correio electrónico no mercado negro, quer seja através de *dealers* orientados para o mercado *spam*, ou no processo de aquisição de listas de endereços a um prestador de serviços legítimo ao qual deu o seu endereço de correio electrónico na compra de algum serviço ou durante o registo em algum *site*/serviço na Internet.

Outra das técnicas utilizada para ***descobrir*** endereços de correio electrónico na Internet é denominada por ***harvesting*** que consiste em pesquisar, de forma insistente e automatizada, *sites web*, arquivos de fóruns ou listas de discussão, entre outros, em busca de endereços de correio electrónico. Na realidade, o *spam* é um roubo de recursos e informações pessoais de todos nós!

As categorias mais comuns de **spam, considerando o seu conteúdo e objectivos, podem ser classificadas em três grupos distintos:**

- **Boatos e Correntes:** Este tipo de *spam*, sendo o de maior dimensão e impacto, apresenta uma característica fundamental: a mensagem solicita que seja enviada para todas as pessoas que conhece. O conteúdo, na generalidade dos casos, refere-se a histórias falsas ou completamente desactualizadas. Para atingir seus objectivos de rápida propagação, os boatos e correntes apelam para diversos métodos de *engenharia social*.

  Os **boatos**, ou vulgarmente denominadas de ***hoaxes***, são textos que contam histórias alarmantes e falsas, que absorvem a atenção do leitor, e instigam a continuar a sua divulgação massiva. Geralmente, o texto começa com frases apelativas do género: "***envie este e-mail a todos os seus amigos...***". Algumas categorias comuns de boatos são os que apelam para a necessidade que o ser humano possui de ajudar o próximo, como exemplo podemos considerar a descrição de casos de crianças com doenças graves, ou histórias de tráfego de órgãos humanos. Outras categorias de boatos são aqueles que difamam empresas ou produtos, prometem brindes ou realização de dinheiro fácil. Alguns exemplos referem-se à existência de certas substâncias cancerígenas em determinados produtos, ou a distribuição gratuita de telefones celulares, de viagens gratuitas à Disneyworld.

  As correntes ou ***chain-letters*** são textos que estimulam o leitor a enviar várias cópias a outras pessoas, gerando um processo contínuo de propagação. São muito semelhantes aos boatos, mas o mecanismo utilizado para incentivar a propagação é um pouco diferente, estando associada a ***promessas*** de sorte e riqueza aos que não as interrompem e anos de má sorte e desgraça aos que se recusam a enviar **N** cópias de mensagens para **Y** pessoas nas próximas **X** horas!

  Links de Interesse:
  http://hoaxbusters.ciac.org e http://www.Vmyths.com

- **Propagandas:** Esta categoria de *spam* tem o objectivo de divulgar produtos, serviços, novos sites, empresas, etc. Enfim, trata-se de *spam* de propaganda generalizada, que tem vindo a ganhar cada vez mais espaço na Internet, e nas respectivas caixas de correio electrónico de todos nós. A legitimidade deste tipo de propaganda (ou *spam*) pode ser discutível, contudo, uma grande variedade de empresas tem utilizado este recurso para atingir os consumidores no mercado Internet. Ultimamente, houve uma ligeira ***inovação*** nesta categoria de *spam*, tendo alargado seu leque de *alvos* e objectivos a propaganda política em vários países. Sendo a Internet um meio muito fértil para promover oferta comercial, vale a pena ressalvar que, segundo a definição de *spam*, qualquer tipo de propaganda, mesmo que se trate de uma promoção com interesse efectivo, o facto de não ter sido solicitado é na realidade considerado uma mensagem de *spam*.

- **Outros: ameaças, brincadeiras**, etc.: Esta categoria de *spam* apesar de estar relacionada com aspectos que rondam os temas da diversão, piadas de mau gosto ou eventualmente, casos de ameaça, pode ser considerada como *spam*. Existem alguns exemplos correntes relacionados com o envio de mensagens em nome de outra pessoa, divulgando conteúdos ofensivos que podem ir desde o insulto à ameaça directa. Actualmente, a apesar de estar a ser realizado algum trabalho nesta área, ainda não existe uma legislação específica para esta categoria de *spam*.

Uma das técnicas mais utilizadas pela comunidade ***spammer*** de envio e promoção de *spam* pela Internet, baseia-se na **utilização de sistemas secundários, vulgarmente denominados por *zombies*, que após terem sido comprometidos, são utilizados como *motores* de *spam* sem a autorização e conhecimento do proprietário.** Contudo, esta situação, aliada ao próprio envio de *spam*, é considerada, perante a legislação actual como **crime informático**. Para além da actividade criminosa de envio de *spam*, ainda existe uma agravante adicional, no acesso não autorizado com posterior utilização ilícita de um sistema alheio.

Outra situação perigosa ainda em actividade na Internet, refere-se ao ***phishing/scam***, considerado como **uma categoria de *spam* que copia e simula a aparência de *sites web* ou empresas legais, solicitando em seu nome informações sobre o cibernauta**. Embora os últimos dados estatísticos refiram que cada vez menos pessoas respondem a mensagens não solicitadas (ou *spam*), ainda existe um grande número de cibernautas que o fazem. O objectivo prende-se com a angariação de informação pessoal de todos nós, como as nossas *passwords*, dados de cartão de crédito, conta bancária... ou seja, **se no início, o *spam* era apenas um incómodo, hoje, também *produz* espiões e burlões.**

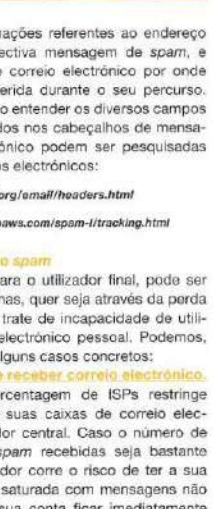
Em termos históricos, e durante os primeiros anos, o alvo principal da comunidade ***spammer*** baseava-se essencialmente em servidores de correio corporativo no mundo empresarial, através de servidores vulneráveis e comprometidos para o efeito. No entanto, com o aumento substancial da largura de banda no meio doméstico, e após o reforço da segurança e monitorização dos servidores empresariais, fizeram com que houvesse uma inflexão estratégica na escolha dos alvos de ***spamming***, colocando os **utilizadores domésticos, nomeadamente aqueles com larguras de banda elevadas, como alvos apetecíveis para a comunidade *spammer*.**

O facto de serem sistemas domésticos fáceis de atacar e comprometer, sem qualquer solução de segurança fiável, que apresentam na sua generalidade endereço IP dinâmico, dificultando o processo de ***tracking*** posterior, condicionam o contexto actual do *spam* estar a ser difundido na sua maioria através deste perfil de sistemas/utilizadores *caseiros*.

Como Combater o spam?

Remando insistentemente contra a maré! A luta contra o *spam* é, por enquanto, inglória... Legislação, filtros, comunidades *anti-spam*, listas negras, bloqueio de domínios associados a *spammers*, envolvimento de governos e empresas, compromisso de utilizadores e provedores de serviço, consórcios judiciais, nada disso parece poder conter a *praga* do *spam*... **A minha recomendação passa por implementar uma combinação devidamente estruturada de vários destes factores**: legislação, tecnologia, educação e melhores práticas para tentar mitigar o impacto do *spam* nas nossas vidas. Apesar da comunidade de *spammers* estarem constantemente a evoluir as suas sofisticadas técnicas de envio ilícito de mensagens de correio electrónico, ainda é possível combater essa *praga* digital. **Aqui vão algumas dicas úteis:**

- Proteja o seu endereço de correio electrónico. Não o divulgue em locais de muito acesso como listas de discussão, fóruns, salas de *chat* ou mesmo no seu site pessoal.
- Utilize ferramentas apropriadas para a filtragem das mensagens de *spam* recebidas na sua caixa de correio electrónico. O provedor de Internet (ISP) tem a responsabilidade de garantir soluções de filtragem de *spam* nas caixas de correio em vigor, portanto, exija essa qualidade junto de quem de direito.
- Nunca responda a mensagens de correio electrónico que não tenha sido previamente solicitado. Isto, apenas indicará, para o remetente (*spammer*), que o seu endereço de correio electrónico é válido, e que poderá ser inscrito em listas de *spam*.
- Evite aceder a endereços electrónicos que não conheça ou confie, pois pode servir para confirmar a veracidade do seu endereço de correio electrónico.
- Nunca reenvie mensagens de *spam* como as "famosas" *correntes*. Para além de validar e publicar o seu endereço de correio electrónico para o mundo, servirá para aumentar o tráfego de *spam* na Internet.
- Evite abrir mensagens de correio electrónico cujo endereço ou nome do remetente não seja conhecido. Geralmente, e no intuito de atrair a atenção e curiosidade de quem recebe, este tipo de *spam* intitulado com temas do género: **"Como vai você?"**, **"Urgente e Confidencial"**, **"Chance imperdível!"**, entre outros.
- Evite guardar ou abrir ficheiros executáveis. Este tipo de ficheiros normalmente possui a extensão ***.exe*** ou ***.com***, e pode instalar alguma aplicação maléfica (*worm*, *vírus*, *spyware*, *trojans*, etc.) no seu sistema.



- Recomenda-se não responder a qualquer mensagem de *spam*, mesmo que seja para solicitar a remoção do seu endereço de correio electrónico da lista de endereços de *spam*. Geralmente, este é um dos métodos que os *spammers* utilizam para confirmar a veracidade, validade e titular do respectivo endereço de correio electrónico.
- Ter imenso cuidado na navegação em *sites* desconhecidos. Evite registar o seu endereço de correio electrónico em *sites* de teor pouco recomendável ou de alguma desconfiança.

Para aprofundar o tema, podem ser encontradas referências para diversas ferramentas de filtragem de mensagens de *spam* nos seguintes endereços electrónicos:

Spam e-mail blocking and filtering:
http://spam.abuse.net/userhelp/#filter
Anti-Spam Yellow Pages:
http://www.antispamyellowpages.com

Para quem devo reclamar quando receber uma mensagem de *spam*? Esta pergunta é realçada quando a nossa caixa de correio está completamente saturada de *spam*, contudo, no intuito de combater esta *praga digital*, é recomendável que se efectue sempre uma reclamação directa para os responsáveis da rede de origem da mensagem de *spam*. Se esta rede possuir uma política de utilização minimamente aceitável, o utilizador que enviou o *spam*, ou seja, o *spammer*, poderá receber as penalidades previstas por lei. Porém, e na maioria das situações, é difícil conhecer a real origem das referidas mensagens de *spam*. Os *spammers* costumam enviar as suas mensagens de *spam* através de sistemas vulneráveis a "*mail relay*", que permitem que terceiros utilizem o seu serviço de correio para enviar as referidas mensagens de *spam* sem a sua autorização ou conhecimento. Caso seja este o cenário, a reclamação servirá para alertar os seus responsáveis do sucedido, e qual o estado de segurança em que se encontra a sua infra-estrutura tecnológica responsável pelo serviço de correio electrónico. Além de enviar a reclamação para os responsáveis da rede, procure manter o endereço de correio ***mail-abuse@cert.pt*** em conhecimento nas reclamações efectuadas. Deste modo, o CERT.pt pode manter dados estatísticos sobre a incidência e origem do *spam* em Portugal e, da mesma forma, identificar servidores e domínios de correio electrónico vulneráveis que têm vindo a ser abusados por *spammers*. Outra questão que se coloca de imediato, está relacionada com a informação que se deve incluir numa reclamação de *spam*. Para que os responsáveis de rede possam identificar a origem de uma mensagem de *spam* é necessário que seja enviada a mensagem recebida, devidamente acompanhada pelo seu cabeçalho completo (*header*). É precisamente no cabeçalho de uma mensagem de correio electrónico que estão armazenadas as informações referentes ao endereço IP de origem da respectiva mensagem de *spam*, e quais os servidores de correio electrónico por onde a mensagem foi transferida durante o seu percurso. Informações sobre como entender os diversos campos normalmente encontrados nos cabeçalhos de mensagens de correio electrónico podem ser pesquisadas nos seguintes endereços electrónicos:

Reading Email Headers:
http://www.stopspam.org/email/headers.html
Tracking Spam:
http://www.claws-and-paws.com/spam-l/tracking.html

Impacto traduzido pelo spam

O impacto do *spam*, para o utilizador final, pode ser traduzido de várias formas, quer seja através da perda de tempo útil, quer se trate de incapacidade de utilização do seu correio electrónico pessoal. Podemos, como exemplo, referir alguns casos concretos:

- **Incapacidade de receber correio electrónico.** Uma grande percentagem de ISPs restringe a dimensão das suas caixas de correio electrónico no servidor central. Caso o número de mensagens de *spam* recebidas seja bastante elevado, o utilizador corre o risco de ter a sua caixa de correio saturada com mensagens não solicitadas, e a sua conta ficar imediatamente bloqueada pelo próprio ISP. Ou seja, o utilizador deixará de receber correio electrónico, até que a sua caixa de correio seja devidamente *limpa* do *spam* recebido anteriormente. Enquanto isso, todas as suas mensagens de correio recebidas legitimamente serão devolvidas ao remetente.
- **Gasto desnecessário de Tempo útil.** Para cada mensagem de *spam* recebida, o utilizador necessita de gastar um determinado tempo para ler, identificar e classificar a mensagem como *spam*, e removê-la da sua caixa de correio electrónico.
- **Aumento de Custos.** Independentemente de qual o acesso à Internet utilizado, quem suporta o esforço financeiro pelo envio de *spam* é quem o recebe em última instância. Como exemplo, um utilizador que acede à Internet através de um modelo de acesso "pague o que gasta", cada mensagem de *spam* que recebe, representa um custo adicional na sua factura mensal.
- **Perda de Produtividade.** Para quem utiliza o correio electrónico como uma ferramenta profissional, o facto de receber mensagens de *spam* aumenta consideravelmente o tempo dedicado à tarefa de leitura e filtragem do seu correio electrónico. Da mesma forma, e por falta de tempo, ainda existe a possibilidade de mensagens de correio importantes não serem lidas, ou serem lidas com atraso devido ao impacto do *spam* no tempo necessário para gerir o correio electrónico.
- **Conteúdo Impróprio ou Ofensivo.** A grande maioria do *spam* é enviada para listas de endereços de correio electrónico aleatórios e sem qualquer controlo de quem é realmente o seu destinatário. Como tal, é provável que alguns utilizadores recebam mensagens de *spam* com conteúdo que considerem impróprio ou ofensivo. Como exemplo, podemos considerar crianças ou menores de idade, profissões de cariz político ou público, etc.
- **Prejuízos Financeiros causados por Fraude.** O *spam* tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o utilizador a aceder a *sites web* clonados de instituições financeiras ou a promover a instalação de vírus ou aplicações maliciosas desenvolvidas com o objectivo de roubar dados pessoais e financeiros. Este tipo de *spam* é conhecido como *phishing*. O utilizador pode sofrer graves prejuízos financeiros e pessoais, caso forneça as informações solicitadas ou execute as instruções apresentadas neste tipo de mensagem fraudulenta.

Tal como na perspectiva dos utilizadores finais, o *spam* provoca graves problemas, quer financeiros quer institucionais, aos ISPs de todo o mundo. Podemos considerar alguns casos específicos de impacto do *spam* sobre entidades empresariais e/ou ISPs, tais como:

- **Impacto na Largura de Banda Disponível.** Para as empresas e ISPs o volume de tráfego adicional gerado pelo *spam* obriga-os a aumentar consideravelmente a capacidade dos seus *links* de acesso à Internet. Devido ao custo dos *links* de acesso serem elevados, constatamos que os lucros do ISO são efectivamente atingidos com este factor. É comum os ISPs reflectirem esse incremento de custos nos utilizadores finais.
- **Utilização dos Servidores.** Os servidores de correio dedicam uma grande percentagem do seu tempo de processamento a gerir o volume adicional de mensagens não solicitadas. Além disso, o espaço de armazenamento, ocupado por mensagens de *spam* recebidas pelos utilizadores é considerável.
- **Inclusão em Listas de Bloqueio.** O ISP que represente utilizadores envolvidos em casos de *spam* pode ter sua rede pública incluída em listas de bloqueio internacionais (RBL).

  Esta inclusão poderá prejudicar o recebimento de correio electrónico por parte de todos os seus clientes/utilizadores e, eventualmente, ocasionar a perda de alguns do seus clientes.
- **Investimento em Recursos Humanos e Equipamentos.** Para lidar com esta *praga*, e problemas associados, os ISPs necessitam de recrutar equipas técnicas especializadas na vertente de segurança, e adquirir equipamentos e soluções de análise e filtragem de *spam*. Esse investimento implica custos adicionais ao ISP.

Todos são alvo de *spammers*! E a *praga* chega a atingir crianças ou menores de idade. Um estudo realizado em Junho pela *AppliedResearch* para a Symantec ouviu mil crianças e jovens entre os sete e dezoito anos de idade, oriundas dos Estados Unidos, e constatou que quatro em cada cinco recebem *spam* com material considerado impróprio. Além disso, 60% dos entrevistados dizem receber uma grande quantidade de anúncios de sorteios e promoções comerciais; 62% já receberam *spam* com serviços de encontro e namoro e, 47% receberam mensagens com endereços electrónicos para sites pornográficos. Da mesma forma, os ISPs também sofrem com a carga adicional de mensagens de *spam* e com as reclamações dos seus clientes. A Yahoo alertou para o crescimento de 40% no volume de mensagens de *spam* entre Janeiro e Agosto. A empresa disse também que o número médio de relatórios de *spam* é de 700 mil mensagens de *spam* por dia. Em Março, o porta-voz da AOL, Nicholas Graham, relatou que os filtros de *software* da companhia teriam eliminado 1 bilhão de mensagens de *spam* num único dia. Em recente reportagem, a Microsoft declarou que 80% do tráfego de correio electrónico em todo o mundo está relacionado com *spam*.

O spam como Negócio

Será o *spam* um bom negócio? No início do ano, o site Wired News publicou uma reportagem propondo um "*mergulho no mar do spam*". A revista escolheu ao acaso 75 entre as mensagens de *spam* que teria recebido nos últimos dias, e respondeu às respectivas mensagens pedindo mais informações. A primeira constatação a retirar, prende-se com a ideia de que responder a *spam* resulta sempre, e incondicionalmente, em mais *spam*. Dos *spammers* pesquisados, 56% nunca responderam às mensagens enviadas. Outros resultados da pesquisa: 16% dos *spam* eram fraudes descaradas, 11% deles geraram mensagens de erro dos servidores comunicando a inexistência do endereço e 17% retornaram respostas com o que pareciam ser ofertas legítimas de produtos ou serviços comerciais.

Se o *spam* é um facto constatado e reconhecido internacionalmente, e se já existem soluções de segurança para o combater, porque será que esta *praga digital* não pára de crescer por todo o mundo? Está obviamente relacionado com o lucro do negócio originado pelo próprio *spam*!

O ano passado, uma falha de segurança num *site web* gerido pelos vendedores de uma pílula de aumento do pénis, expôs um registo de pedidos da *Amazing Internet Products*. Em quatro semanas, seis mil pessoas encomendaram o suplemento à base de ervas anunciado novas mensagens de *spam*, a 50 dólares cada embalagem. A maioria das pessoas encomendou duas, mas teve quem comprasse quatro e, até mesmo seis caixas da pílula que prometia um aumento de no mínimo 7,6 centímetros. Considerando que a companhia teve um gasto ínfimo para enviar as suas mensagens de *spam* e, paga muito pouco aos parceiros de que dispõe, a margem de lucro é impressionante!

Outra história emblemática, é a de Sanford Wallace, que se tornou bastante conhecida na Internet nos anos 90, devido ao facto da sua empresa de marketing, a Cyber Promotions, enviar cerca de 25 milhões de mensagens de *spam* por dia. Estima-se que, na época, "*Spamford*", como foi apelidado, fosse o responsável por 80% do *spam* que existia na Internet. Em 1998, depois de muitos processos, ele mudou a sua forma de actuar mas, tentou manter o seu negócio, agora trabalhando com propaganda enviada com autorização do utilizador. Prosperou bastante, até que a crise das *dot.com* colocou o seu negócio em falência absoluta. Convencido da ilegalidade do negócio, Sanford mudou totalmente de vida. Actualmente, é dono de dois clubes nocturnos em New Hampshire.

O futuro do spam

Em Abril deste ano, a AOL, Microsoft e a Yahoo anunciaram uma parceria estratégica contra o *spam*, no desenvolvimento de um trabalho conjunto com o objectivo de combater o *spam* na Internet, impedir a criação de endereços de correio electrónico fraudulentos e, finalmente, retomar o controlo do universo do correio electrónico. Os países também se organizaram nesse sentido, modernizando e endurecendo as suas legislações locais. Nos Estados Unidos, a lei aprovada recentemente pelo Senado, pode causar ao *spammer* multas até 1 milhão de dólares. Da mesma forma, e acentuando os países da comunidade europeia, têm vindo a desenvolver esforços no intuito de combater insistentemente o *spam* no mundo. **O movimento *anti-spam* é mundial, como a própria *praga* do *spam*...**

Wikipédia, a enciclopédia livre:
http://pt.wikipedia.org/wiki/Spam
Fight Spam on the Internet:
http://spam.abuse.net/
AntiSpam:
http://www.antispam.br/
EliminarSpam.com:
http://www.eliminarspam.com/
Spam Laws:
http://www.spamlaws.com/

***Bruno Castro**
Director Geral da VisionWare
Mestre em Engenharia Informática (Segurança da Informação)
bcastro@visionware.pt