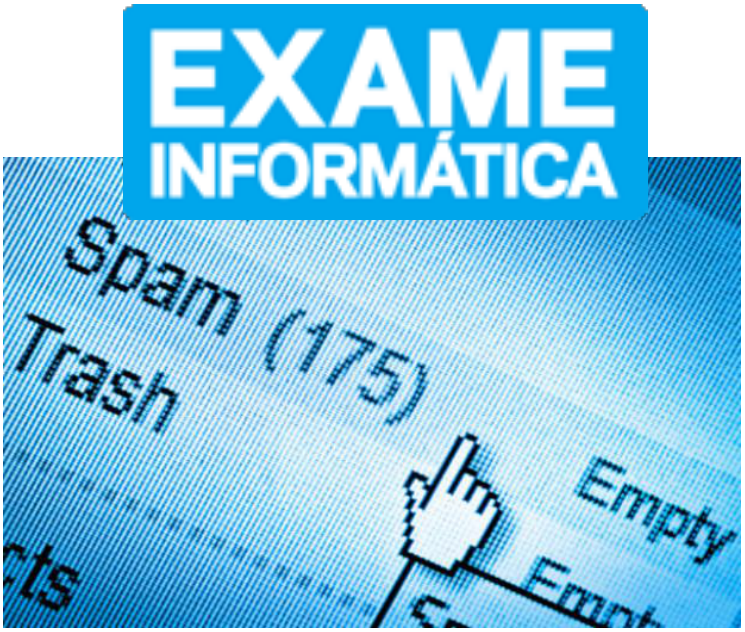
Em Portugal, há 200 servidores prontos a serem usados por spammers

No início de 2013, a Dognaedis contabilizou mais de 200 servidores de e-mail a operar em Portugal que podiam ser controlados por spammers ou até hackers que pretendam lançar ataques de phishing através de e-mails.



O número pode ter subido ou descido nos meses que se seguiram - mas no início de 2013 havia mais de 200 servidores de e-mail a operar em Portugal que, devido à má configuração, podiam ser usados por spammers... ou mesmo hackers.

Os dados apurados pela empresa Dognaedis: através de ferramentas de rastreio dos cerca de cinco milhões de números IP usados em Portugal, a empresa de Coimbra detetou, no início de 2013, mais de 200 servidores mal configurados que permitem que um spammer re-envie correio eletrónico não solicitado para milhares de internautas e dissimular a autoria do envio de spam.

João Gouveia, diretor Técnico da empresa de segurança eletrónica AnubisNetworks, relativiza a ameaça, mas confirma que os open relays são uma realidade no País: «Em Portugal, podemos estimar que esse número andará na casa das poucas centenas, ou mesmo dezenas, embora possa sofrer alterações à medida que as empresas corrigem os problemas de configuração». Francisco Nina Rente também confirma que o número de open relays é «mutável», e está dependente do estado de alerta dos proprietários das máquinas.

Na gíria da informática, estes servidores mal configurados são conhecidos como open relays. Francisco Nina Rente, líder da empresa, explica os riscos que correm estas máquinas: «São servidores mal configurados, que podem ser usados para re-enviar spam, sem que se saiba quem é que é o spammer. Além disso, esta má configuração deixa a porta aberta para todos os vetores de ataque que são suportados pelo spam, como os e-mails de phishing ou as diversas formas de disseminação de malware».

Tendo em conta o total de números IP usados em Portugal, o número de open relays poderá ser encarado como reduzida. Mas a Dognaedis acrescenta alguns dados que permitem ter uma noção mais aproximada das proporções que esta ameaça pode ter: «se cada um destes servidores for usado para enviar 1000 ou 2000 e-mails por minuto, aí compreendemos que se trata de um número considerável».

Francisco Nina Rente sublinha que o facto de ter encontrado servidores de e-mail mal configurados não significa que a Dognaedis saiba quantos desses servidores estão a ser usados, atualmente, para atividades menos lícitas. «Só os donos dos servidores ou, eventualmente, os operadores de telecomunicações podem saber o que fazem esses servidores. Com a nossa ferramenta apenas podemos dizer se o servidor está ou não vulnerável. Se tentássemos saber o que andam a fazer esses servidores arriscávamo-nos a cometer uma ilegalidade».

João Gouveia desvaloriza o grau de ameaça causado pelos open relays, lembrando que, foi nos anos 1990 e início de 2000, que a exploração da má configuração dos servidores de e-mail esteve mais em voga. «Hoje, as técnicas de envio de spam focam-se acima de tudo na utilização das botnets, recorrendo também às contas comprometidas, ou servidores comprometidos (através da exploração de vulnerabilidades)», explica quando questionado pela Exame Informática.

O responsável da Anubis relaciona a perda de importância dos open relays com a sofisticação crescente das tecnologias anti-spam: «com a evolução dos mecanismos anti-spam, um servidor que esteja em estado de open relay, muito rapidamente é abusado, e como consequência detetado e bloqueado por listas negras (do spam). O que faz com que este método não seja propriamente eficiente para quem quer enviar spam».

A crescer desde 2009

A exploração de open relays pode já não estar na moda entre os spammers, mas os números apurados pela Dognaedis revelam que também os departamentos de informática portugueses não dão grande importância a este tipo de vulnerabilidade. No final de 2009 foram detetados 78 open relays; e no final de 2010 eram 91.

Apesar de eficiência questionável no que toca ao spam, os open relays deixam em aberto um manancial de estratagemas e iniciativas de legalidade duvidosa, a que provavelmente nenhum internauta minimamente avisado gostaria de estar associado. De quem são estes servidores de e-mail? João Gouveia dá uma ideia: «Tipicamente os servidores que estão em estado de open relay pertencem a empresas ou organizações perfeitamente legítimas, normalmente de pequena dimensão. Este estado é normalmente provocado por falhas de configuração que resultam, muitas vezes, da intervenção de pessoas não qualificadas que tentam instalar e configurar um servidor de Email pela primeira vez».Francisco Nina Rente tem uma opinião similar sobre a o que está na origem dos open relays disponíveis atualmente em Portugal: «São falhas fáceis de resolver. Tudo leva a crer que não são servidores de spammers porque estão associados a domínios a registar».