

São Paulo, 11 de julho de 2007

## **Projeto SpamPots revela números surpreendentes sobre spam no Brasil**

*Iniciativa inovadora da CT-Spam, mantida pelo CGI.br/NIC.br, mensura o abuso de máquinas de usuários finais para o envio de spam*

O Comitê Gestor da Internet no Brasil, CGI.br ([www.cgi.br](http://www.cgi.br)), através da Comissão de Trabalho Anti-spam (CT-Spam), apresenta os resultados preliminares do Projeto SpamPots, iniciativa pioneira que utiliza honeypots de baixa interatividade na obtenção de métricas sobre o abuso de redes de banda larga para o envio de spam. Coordenado e desenvolvido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT.br ([www.cert.br](http://www.cert.br)) do Núcleo de Informação e Coordenação do Ponto BR, NIC.br ([www.nic.br](http://www.nic.br)), o projeto contabilizou, em 325 dias de atividade, mais de 370 milhões de mensagens.

De acordo com Cristine Hoepers, analista de segurança do CERT.br, nos últimos anos, as reclamações sobre spams enviados através do uso indevido de máquinas brasileiras com proxies abertos ou proxies instalados por códigos maliciosos têm crescido continuamente, chegando a 55% do total de reclamações recebidas no último mês de junho. Porém, até o momento, praticamente nenhum dado era conhecido sobre a natureza, a origem ou destino desse tipo de spam. “É muito importante a obtenção de dados que nos permitam entender melhor o perfil do abuso de proxies no Brasil, de modo a facilitar a proposição de formas de prevenção mais efetivas”, explica.

Os resultados preliminares do projeto revelam números surpreendentes. Além de um total de 370.263.413 e-mails coletados em 325 dias, o número de destinatários seria de 3.287.153.093, o que representa uma média de 8,9 destinatários por spam. No total, foram identificados 160.512 IPs únicos de 157 países diferentes, que enviaram em média 2,3 mil mensagens cada um.

A lista dos 10 países que mais abusam do Brasil, de acordo com os resultados preliminares, traz Taiwan em primeiro lugar, com 281.601.310 e-mails capturados, ou 76% das ocorrências. China vem em segundo lugar, com 58.912.303 e-mails ou 16% do volume analisado. Estados Unidos, Canadá, Coreia, Japão, Hong Kong, Alemanha, Brasil e Panamá são os outros países que aparecem na listagem, e que juntos somam menos de 8%.

### **Arquitetura**

Com foco nas redes ADSL e cabo nas versões doméstica e empresarial, o projeto utiliza 10 honeypots de baixa interatividade, ou seja: computadores configurados de modo a apenas emular determinados sistemas operacionais e serviços. “Quando um spammer interage com um destes honeypots, ele não está interagindo diretamente com o sistema, mas sim com um programa que emula suas características, como sistema operacional e versões de aplicativos”, explica Klaus Steding-Jessen, analista de segurança do CERT.br.

Um spammer que tentar abusar de um destes honeypots para o envio de spam estará, na verdade, interagindo com programas projetados para fazê-lo acreditar que consegue enviar seus e-mails. Deste modo, nenhum spam foi realmente enviado aos destinatários, mas apenas coletado para análise por um servidor central.

### **Trabalhos Futuros**

O projeto inclui diversas atividades, ainda em andamento, e trará, em poucos meses, análises mais detalhadas do problema, por meio de técnicas de mineração de dados. O objetivo é determinar a ocorrência de padrões envolvendo idiomas, pontos de origem e conteúdo das mensagens, além de gerar algoritmos para melhor caracterização de spams e que possam auxiliar o processo de filtragem.

Geração de relatórios públicos com recomendações de melhores práticas para provedores de serviços de banda larga e um acordo de cooperação internacional com grupos de tratamento de incidentes de outros países também fazem parte das ações programadas para a segunda fase do projeto. “Queremos ter uma visão mais global do problema e propor ações efetivas no combate ao spam no país”, diz Klaus.

**Para ter acesso ao material mais detalhado do Projeto SpamPots, acesse:**  
<http://www.cert.br/docs/whitepapers/spampots/>

### **Sobre o Núcleo de Informação e Coordenação (NIC.br)**

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br ([www.nic.br](http://www.nic.br)) é uma entidade civil, sem fins lucrativos, criada para implementar as decisões e projetos do Comitê Gestor da Internet no Brasil — CGI.br ([www.cgi.br](http://www.cgi.br)), que é o responsável por coordenar e integrar as iniciativas de serviços da Internet no país. O NIC.br responde pelo registro de nomes de domínio — Registro.br ([www.registro.br](http://www.registro.br)), pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br ([www.cert.br](http://www.cert.br)), pela implantação e operação dos Pontos de Troca de Tráfego — PTT.br ([www.ptt.br](http://www.ptt.br)) e pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação —

CETIC.br ([www.cetic.br](http://www.cetic.br)), cujo objetivo é produzir e divulgar informações e estatísticas sobre a disponibilidade e o uso da Internet no país.

### **Sobre o CERT.br**

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Mantido pelo Comitê Gestor da Internet no Brasil, o grupo é responsável por receber, analisar e responder incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil. As estatísticas de spam do CERT.br (<http://www.cert.br/stats/spam/>) fornecem uma visão do problema do spam em redes brasileiras, por meio da análise das reclamações recebidas.

Para mais informações, acesse: [www.s2.com.br](http://www.s2.com.br) ou [www.nic.br](http://www.nic.br) ou <http://www.cert.br/>

**Empresa:** Núcleo de Informação e Coordenação (NIC.br)

**Fonte:** Mariana Balboni, gerente de comunicação

### **Contatos para a imprensa:**

**S2 Comunicação Integrada** - <http://www.s2.com.br>

**PABX:** (11) 3457.0200 / **Fax:** (11) 3457-0222

Veronica Cassavia – [veronicac@s2.com.br](mailto:veronicac@s2.com.br)

Telefone: (11) 3457-0226

José Luiz Schiavoni (MTb 14.119) - [joseluiz@s2.com.br](mailto:joseluiz@s2.com.br)