Insegurança desafia a internet
Henrique Faulhaber

A utilização cada vez mais ampla de tecnologias da informação e da comunicação vem acompanhada do crescimento de vulnerabilidades na área de segurança. Essa questão figura entre as grandes prioridades de governos, organismos internacionais e empresas, pois a insegurança no ciberespaço atingiu proporções tão alarmantes que está ameaçando o próprio desenvolvimento da sociedade da informação.

As tentativas de fraudes eletrônicas reportadas ao Grupo de Resposta a Incidentes de Segurança, mantido pelo Comitê Gestor da Internet no Brasil (CGIBr) cresceram 74% no ultimo trimestre, reforçando o alarme de que os ataques às redes estão se tornando cada vez mais perigosos também em nosso país.

É necessária a conscientização dos usuários e administradores de redes sobre os riscos incorridos no uso da internet e sobre as melhores práticas aplicáveis de segurança para se conseguir inverter a tendência de crescimento de ameaças eletrônicas com que nos defrontamos.

Da mesma forma como lidamos com insegurança urbana, precisamos saber como devemos nos comportar nos atuais tempos perigosos da internet. Os especialistas em segurança da informação recomendam manter atualizados os programas de antivírus e sistemas operacionais, instalar software "firewall" de segurança para bloquear acessos externos, e nunca abrir um site de internet ou e-mail suspeito.

Infelizmente tomar essas precauções básicas é impraticável para a maioria dos milhões de internautas nacionais, pois à distância entre o mundo cibernético real e o ideal é enorme. Na internet existem milhões de sistemas operacionais desatualizados e com falhas de segurança, micros sem nenhum antivírus, usuários que clicam em qualquer link sem a menor cerimônia, e poucos programas de bloqueio de acesso indesejado instalados. Essa situação é agravada com a popularização do acesso rápido a internet que está permitindo que um número cada vez maior de empresas e pessoas fiquem conectadas em tempo integral na rede tornando-se um alvo fácil e desejável para os "hackers" de todo o mundo.

Os vilões nessa história infelizmente não são mais somente a legião de adolescentes em busca de fama instantânea e satisfação técnica por invadir sistemas. Os ataques mais perigosos na internet já têm características de crime organizado, uma vez que o aumento da incidência de fraudes bancárias (obtida através da obtenção de senhas), os casos de extorsão contra sites no exterior ameaçados de serem colocados fora do ar, a pirataria, e a espionagem envolvem grandes valores financeiros. Uma das mais recentes ameaças a segurança das redes são as "Botnets". Os micros infectados por esse novo tipo de vírus (bots) formam redes de computadores "zumbis" que são comandados simultaneamente por seus invasores para enviar mensagens indesejadas (spam), colocar sítios fora do ar e promover fraudes.

Os avanços da rede estão sendo ameaçados

O fato mais grave relacionado as botnets, que as caracteriza como uma ação de crime organizado segundo a agencia "Reuters", é que já existem milhões de PCs controlados dessa forma e que algumas redes de micros infectados podem ter até trinta mil equipamentos e são alugadas para quadrilhas por pelo menos US$100 por hora.

Os criminosos eletrônicos usam essas redes de máquinas "escravas", de maneira análoga àquela que os ladrões tradicionais usam carros roubados para fazer seus assaltos. A prática comum de fazer "spam" através dessas maquinas "invadidas" mostra que o correio eletrônico mal intencionado é a principal ferramenta do crime cibernético, e por isso tem de ser combatido com rigor especial.

No Brasil a recente ação da Policia Federal na operação "Cavalo de Tróia" em que foi presa uma quadrilha nacional de fraudadores de contas bancárias demonstra que crimes eletrônicos estão realmente se tornando mais comuns nos país, mas que eles podem ser rastreados e os culpados punidos.

A comunidade de especialistas de segurança da informação das empresas privadas, universidades, provedores de acesso e governos estão permanentemente discutindo esse tema, e trabalhando articuladamente para fazer frente a essas ameaças.

Uma iniciativa importante nesse sentido é o Consórcio Brasileiro de Honeypots, que é mantido por instituições (CGIBr, universidades, bancos, empresas de telecomunicação, provedores) e que tem como objetivo aumentar a capacidade de diagnosticar incidentes de segurança, determinar tendências de ataques, detectar servidores comprometidos, e detectar redes infectadas por vírus.

Este projeto consiste em instalar pontos "escondidos" de coleta de informação de segurança em redes distintas da Internet brasileira, de forma a obter amostragem dos ataques reais que sendo feitos diariamente aos usuários.

Uma vez identificada à atividade maliciosa, é verificado se a origem do ataque ocorreu no país ou no exterior, é determinado o contato do administrador da rede da onde ocorreu o ataque, e é feita a advertência do incidente para buscar providencias.

As ameaças de segurança são um dos principais desafios de governança da internet. Este é um problema internacional que precisa ser atacado por meio da identificação de incidentes, conscientização da sociedade, e do trabalho coordenado de especialistas, empresas e governos.

Valor Econômico – 24 nov. 2004, Empresas & Tecnologia, p. B2