Proteja-se!

Secretaria de Tecnologia da Informação e Comunicação – **SETIN**
Coordenadoria de Apoio à Governança e Gestão de TIC – **CGOV**
Seção de Gestão da Segurança da Informação – **SGSI**

Principais Ameaças (*Mail Bomb*, *Smurf* e *Phreaking*)

Nº 25, agosto de 2019

Dando continuidade ao tema de ameaças, este boletim traz novos conceitos.

Mail Bomb é uma técnica na qual o atacante envia um grande fluxo de mensagens eletrônicas com o propósito de encher a caixa postal de e-mail e sobrecarregar o equipamento servidor de correio eletrônico. O objetivo é realizar a negação de serviço, em outras palavras, tornar o serviço de e-mail indisponível.

Smurf é um tipo de ataque que tem por objetivo tornar indisponível determinado serviço. O agressor envia uma rápida sequência de solicitações de *ping* (um teste para verificar se um servidor da internet encontra-se acessível) para um endereço de *broadcast* (que propaga a solicitação). Usando *spoofing**, o cracker faz com que o servidor de *broadcast* encaminhe as respostas não para o seu endereço, mas para o da vítima. Assim, a vítima é congestionada pelas respostas do servidor, podendo ocorrer negação de serviço.

Phreaking consiste no uso indevido de linhas telefônicas, fixas ou celulares através da exploração dos ativos de telecomunicações, como equipamentos e sistemas conectados a redes de telefonia públicas. O *cracker** de telefonia que pratica esse tipo de ataque é chamado de *phreaker*, termo que vem da junção das palavras inglesas *phone* e *freak*, ou *phreak*.

O *Phreaking* foi um dos primeiros tipos de fraudes registrados em telecomunicações, tendo ocorrido no ano de 1957, quando a companhia de telecomunicações AT&T foi vítima.

Com a modernização e reforço na segurança das companhias, essas técnicas tornaram-se mais difíceis de serem executadas. Atualmente, é considerada uma atividade bastante elaborada, a qual poucos *hackers* dominam.

* Para mais informações, vide boletim Nº 13.

Importante!

Invasões e ataques de negação de serviços, como é o caso de *Mail Bomb* e *Smurf*, vêm se tornando um problema cada vez mais grave, pois novas técnicas de ataques surgem a todo instante, e as já existentes evoluem para se tornarem cada vez mais eficientes.

A grande dependência e interligação entre as redes, serviços, sistemas e aplicações na internet é um facilitador para as ações dos cibercriminosos.

Os administradores de serviços e sistemas encontram um grande desafio na tarefa de impedirem esses tipos de ataques, já que muitas máquinas ligadas à rede não têm nenhum tipo de proteção e, ainda pior, atuam como amplificadoras para que os ataques se tornem mais poderosos.

Boas práticas de segurança podem ser aplicadas para prevenir que redes e serviços sofram esse tipo de ataque. É necessária a aplicação de soluções técnicas e a adoção de uma postura preventiva: as soluções técnicas ajudam a proteger das ameaças já conhecidas; enquanto a postura preventiva auxilia na prevenção de exploração de outras vulnerabilidades.