Proteja-se!

Secretaria de Tecnologia da Informação - SETIN
Coordenadoria de Gestão da Informação - CGI
Seção de Gestão de Segurança da Informação - SGSI

Principais ameaças (*Backdoors, Man in the Middle, Probing* e *Rootkits*)

Nº 17, fevereiro de 2016

Dando continuidade ao tema ameaças, assunto dos boletins 9, 11, 13 e 15, serão tratados mais quatro tipos: *Backdoors, Man in the Middle, Probing* e *Rootkits*.

Backdoors são programas que têm por objetivo prover acesso aos computadores infectados, sem que haja a necessidade de exploração de alguma vulnerabilidade. Dessa forma, o computador pode ser totalmente controlado à distância sem que o invasor seja notado.

O *backdoor* permite que o invasor acesse o computador sempre que quiser e permite facilmente furto ou manipulação de informações.

Man in the Middle é uma forma de ataque na qual informações trocadas entre duas partes são interceptadas pelo invasor, possibilitando a alteração dessas informações sem que o usuário perceba. Normalmente esse ataque acontece quando o usuário está acessando o *home banking* de um banco ou instituição financeira, no momento da troca de informações para que as transações sejam efetuadas.

As formas de ataque podem se utilizar de brechas na criptografia, de código malicioso ou de roteador mal configurado, entre outras.

Probing é uma forma de conseguir informações sobre uma rede. Não pode ser considerada uma forma de invasão, mas é uma das técnicas usadas para uma futura invasão através da informação coletada sobre a rede.

Com essa técnica de reconhecimento pode-se descobrir, por exemplo, quais sistemas ou serviços estão ativos em determinado momento em cada estação da rede.

Rootkits são ferramentas utilizadas para esconder a existência de programas ou processos maliciosos dos métodos convencionais de detecção, por exemplo, antivírus. Sempre que o sistema operacional faz a leitura de um arquivo, o *rootkit* intercepta os dados e só permite a leitura de arquivos não infectados.

Importante

Há maneiras bem simples de se ter uma maior proteção contra esses tipos de ataques.

O recomendado é que você não execute programas duvidosos ou desconhecidos, sejam eles recebidos por e-mail ou obtidos na internet, nem acesse sites ou links suspeitos.

Caso você utilize algum programa de acesso remoto, certifique-se de que ele esteja bem configurado, para evitar sua utilização como um *backdoor*.

Procure entrar em sites que tenham o prefixo "HTTPS" e um símbolo de conexão segura, normalmente um cadeado localizado na barra de endereços, além de manter seu navegador sempre atualizado.

Mantenha seu antivírus sempre atualizado e utilize também *firewall*, *antispam* e *antispyware*.

Lembre-se: em se tratando de ameaças, prevenção nunca é demais.

Acesse a Política de Segurança da Informação em http://aplicacao.tst.jus.br/dspace/handle/1939/27977

Na intranet, todos os boletins podem ser acessados em http://autoatendimento.tst.jus.br/index.php?option=com_docman&Itemid=62

Participe! Caso tenha alguma dúvida, sugestão ou crítica envie para sgsi@tst.jus.br