70 - Novembro de 2005

Você já ouviu falar em seqüestro de dados?

Não é por acaso que vemos agora esta expressão aplicada ao ambiente eletrônico. Depois do tradicional seqüestro de pessoas seguido de negociação e resgate, e do seqüestro relâmpago que priva temporariamente a liberdade do individuo até que ele retire quantia de dinheiro suficiente para ser libertado, vemos o mesmo conceito ocorrendo no universo da seguranca informação.

Esta moderna e criativa forma de extorquir dinheiro em meio eletrônico tira proveito do alto nível de conectividade das redes, das fragilidades dos sistemas, da alta produção de informação em meio eletrônico e, na versão mais avançada, da criptografia. A dinâmica do golpe compreende do acesso não autorizado ao computador, ora transferindo dados sigilosos e valiosos da maquina do usuário para a maquina do seqüestrador, ora codificando os dados na própria maquina do usuário através de criptografia forte. Isso feito, o conceito do tradicional seqüestro volta a ser usado, seguido do contato entre o seqüestrador e a vitima em que e negociada uma condição, comumente uma quantia em dinheiro, para que a vitima possa reaver o acesso aos seus dados.

Simples e terrivelmente eficaz. No modelo mais avançado do golpe, os dados sequer são transferidos, copiados ou alterados, são simplesmente protegidos pelo seqüestrador com criptografia forte o suficiente para que só ele tenha acesso, mesmo que a vitima tente quebrá-la por forca bruta. E como um tiro saindo pela culatra ou a tecnologia de seguranca da informação criada para protegê-lo, sendo usada contra você.

Após o fato consumado, não há muito que fazer, pois o poder de proteção da criptografia é matematicamente proporcional à chave criptográfica e algoritmo utilizados e ao poder de processamento dos computadores, que por vezes, inviabilizam qualquer tentativa de quebra por forca bruta em tempo hábil.

Relatos isolados sobre o golpe já surgiram na Europa e na America do Norte em iniciativas amadoras, mas tudo indica que será velozmente difundido nos próximos anos por seu potencial de gerar dinheiro rápido e com relativa baixa exposição do seqüestrador, afinal, ele pode estar em qualquer lugar do mundo, em qualquer rede e em qualquer equipamento conectado a Internet. Acredita-se que o golpe possa se profissionalizar e migrar para o ambiente corporativo onde o valor da informações é maior e o golpe, supostamente mais rentável.

Se existem dicas para minimizar o risco de se tornar uma vitima do seqüestro de dados, elas estão especialmente vinculadas à proteção do sistema, à proteção da conexão Internet, ao comportamento de risco do usuário, evitando a execução de programas suspeitos e o clique em links desconhecidos, por exemplo, e claro, ao desenvolvimento do habito de backup. Chegou mesmo o momento de usar a contra-inteligencia a serviço do usuário.

Marcos Sêmola *é Consulting Business Development da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC e do Computer Security Institute, Professor da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004. Visite www.semola.com.br ou contate marcos@semola.com.br*