95a – Janeiro 2008

Previsão das Principais Ameaças para 2008

Depois de um ano tumultuado e recheado de incidentes de segurança, como de costume, já é possível prever a anatomia de algumas ameaças que se destacarão em 2008. Por isso, é bom já conhecer seu perfil e planejar ações incrementais preventivas.

1. Phishing via Email
   Os golpes aplicados através de email continuarão crescendo, dada a crescente popularidade da ferramenta de correio eletrônico e a alta probabilidade do usuário em acreditar nas mensagens, seus links e arquivos anexados. Os emails falsos chegarão ainda mais próximos do real, bem construídos, abordando temas atuais, e explorando as fraquezas naturais do ser humano.

2. Roubo de Identidade
   As inúmeras interfaces de comunicação online, especialmente as redes sociais, e a necessidade/ingenuidade do usuário em expor detalhes da vida privada farão aumentar os casos de roubo de identidade, o que acaba ocorrendo com a obtenção não autorizada ou a simples adivinhação de senhas de acesso e chaves de identificação.

3. Virus no PC e Celular
   Os worms ou vírus de computador continuarão sua curva de crescimento e especialização, explorando falhas cada vez mais recentes dos sistemas e aplicações e usando especialmente o usuário para levá-los ao ambiente vulnerável. O celular e dispositivos móveis inteligentes começarão a ser alvos de ataques de interrupção de serviço e ataques destrutivos que poderão comprometer os dados armazenados.

4. DDOS SPAM
   As correspondências eletrônicas não autorizadas continuarão crescendo, consumindo seu tempo, seu link Internet, o poder de processamento do seu computador, sua caixa de email e principalmente colocando à prova seus dispositivos de filtragem. Muitos provocarão apenas perda de tempo, mas muitos outros virão com segundas intenções, por vezes escondendo um ataque phishing ou vírus, o que exigirá ainda mais atenção do usuário ao selecionar a correspondência legítima.

5. Golpes via Celular
   Mais recentemente no Brasil e já comumente na Europa e América do Norte, o telefone celular é usado como dispositivo de autenticação e meio de pagamento, por isso, as formas de ataque serão mais modernas e eficazes na tentativa de invadir o equipamento e comandar ações que provoquem desde a perda de informações ao desvio de recursos e, possivelmente, dinheiro. Mensagens estranhas solicitando comandos e ações vão começar a chegar sem aviso prévio, podendo, em um futuro breve, se tornar um SPAM de SMS ou algo parecido.

6. Ataques Wi-Fi
   As redes sem fio Wi-Fi com acesso à Internet se popularizaram em 2007 e na Europa podem sem encontradas em toda parte, muitas vezes, sem a proteção mínima. Por isso, principalmente locais públicos se tornarão um *play ground* para golpistas que procuram equipamentos desprotegidos simplesmente para infiltrar um vírus ou ainda procurar dados sigilosos e senhas que irão trafegar neste ambiente desprotegido.

7. Ataques Bluetooth
   O alto nível de conectitivade oferecido pelos dispositivos móveis, especialmente através da conexão sem fio Bluetooth, serão mais exploradas pelos golpistas já que se popularizaram e representam uma real porta de acesso ao equipamento se não estiver corretamente configurado. Por isso, mensagens indesejadas, simples propaganda e a tranferência não autorizada de dados podem ocorrer.

8. Keylogger Trojans
   O movimento dos cavalos de tróia continua em 2008, especialmente sua capacidade de registrar sem autorização e silenciosamente tudo que é digitado no teclado. Com o aumento dos links de comunicação e a popularização dos pacotes domésticos de *broadband*, as potenciais vítimas tornam-se disponíveis por mais tempo ao longo do dia, dando assim ainda mais tempo para o golpista estudar o alvo, penetrar e monitorar.

9. Hootkits
   Os softwares chegam ao computador do usuário de forma ainda mais veloz e vindo de multiplas origens, seja uma simples atualização automática de rotina do sistema operacional, seja um email com arquivo anexado ou ainda um pacote de atualização de um dos inúmeros *softwares* instalados. Fica, portanto, difícil distinguir o que é legítimo, levando o usuário a autorizar o *download*, a instalação e até mesmo a liberação do pacote através da alteração na regra do *firewall*. Por tudo isso, os *hootkits* irão chegar ainda mais próximos de seus alvos e esconderão códigos maliciosos no sistema operacional comprometendo o seu anonimado.

10. Usuários Desatentos
    Infelizmente os usuários continuarão sendo uma das dez principais ameaças à segurança da informação em 2008. Seja pela falta de uma cultura homogênea de uso, pela complexidade tecnológica dos sistemas, pela alta especialização dos golpes ou simplesmente pela falta de tempo para avaliar cada situação, continuará nas mãos do usuário a decisão de ir em frente, clicar, autorizar, aceitar, executar ou simplesmente ignorar o que, em uma fração de segundo, pode representar a tomada de mais uma dose de risco.

Marcos Sêmola *é IT Compliance Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information*

Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.