

Dia de Pescaria - Phishing e Roubo de Identidade

por Duval A. Costa *

Aqueles cuja idade estiver próxima à minha, lá por volta dos seus quarenta anos, talvez se lem brem de uma marchinha de Carnaval que dizia alguma coisa parecida com:

“Domingo é dia,
De pescaria,
E lá vou,
De caniço e samburá...
Maré está cheia,
Fico na areia,
Por que na areia dá mais peixe que no mar...”

Infelizmente para os usuários de sistemas de correio eletrônico, algumas mudanças importantes ocorreram com relação à letra da marchinha, dado que a “pescaria” acontece todos os dias (não mais apenas aos domingos), o que se alia ao fato destes usuários passarem, eventualmente, de pescadores a “pescados”, sempre que abrem suas caixas postais virtuais, pessoais ou corporativas.

A “pescaria virtual” a que se faz referência neste texto vem a ser a “pescaria e colheita de senhas” (tradução livre do inglês “*password harvesting fishing*” ou simplesmente “phishing”), uma modalidade de ataque bastante comum, a qual tenta comprometer principalmente o sigilo das informações, a divulgação indevidamente informações pessoais ou corporativas.

Este ataque é com posto por um misto interessante entre (i) “Engenharia Social” (uso de técnicas ou métodos de convencimento, utilizados com o intuito de iludir ou ludibriar visando obter informações pessoais) e (ii) “CrimeWare” (como o próprio nome fortemente sugere, uso de “software criminoso” ou de programas de computador cuja intenção é a de auxiliar que crimes sejam cometidos), sendo o principal objetivo de seus autores o de “pescar”, seja, colher ou apropriar-se, sem o conhecimento ou consentimento de seus legítimos proprietários, de informações pessoais ou corporativas, tais como, por exemplo, números de contas bancárias, números de cartão de crédito, números de identificação, tais como RG e CPF, códigos de identificação de usuário – user-ids – e senhas de controle de acesso.

O esquema (do inglês “scam” – o nosso popular golpe ou “conto-do-vigário”) é engenhosamente simples, envolvendo o envio de quantidades industriais de mensagens eletrônicas não solicitadas (os famosos “spams”), muitas vezes escritas em português razoavelmente bom, a listas de endereços de correio eletrônico, obtidas, geralmente, de forma espúrea.

O texto da mensagem, em geral, é escrito de modo a aguçar, de alguma forma, seja cativando, enganando ou pura e simplesmente ameaçando, a curiosidade do leitor, por exemplo dizendo se tratar de um amigo de quem não se tinha mais notícia, de alguém apaixonado (também sabem ser românticos os atacantes), de uma oferta imperdível, de um pedido de cotação urgente de um cliente potencial, de um aviso de uma instituição financeira na qual o leitor tenha conta ou mesmo de um aviso de que o nome do leitor da mensagem estaria em alguma lista de maus pagadores ou coisa que o valha, de modo a convencê-lo a “clique” em um “link” de hipertexto, contido na mensagem, o qual dá acesso a um “site” forjado (falso), porém guardando grande semelhança em relação ao “site” original ou verdadeiro (por exemplo, o “site” da empresa que supostamente tenha enviado a mensagem).

Esta atitude impensada de simplesmente “clique” no “link” contido na mensagem pode levar a que um programa espião (muitas vezes tratado por “spyware”, um “primário” próximo dos vírus, vermes e cavalos de tróia) seja instalado no computador onde a mensagem tenha sido aberta, dado ser o “site” forjado mantido e controlado pelo atacante.

Uma vez instalado, o “programa criminoso” abre o “saco de maldades” preparado por seu autor, passando, dentre outras coisas a monitorar, por exemplo, tudo o que os usuários do computador digitam, que “sites” visitam, que arquivos recebem, enviam e modificam, guardando estas informações pessoais ou corporativas e enviando-as, de tempos em tempos, a locais pré-determinados por seu autor.

Programas mais sofisticados poderão até mesmo instalar um a “porta traseira” (as conhecidas “backdoors”), permitindo que o computador da vítima possa ser controlado remotamente, transformando-o em um computador zumbi (“zombi computer”), legiões inteiras dos quais possam ser comandados a distância por seus “mestres”, tal qual os morto-vivos dos filmes de terror classe B, para atividades variadas e instrutivas, tais como mandar mensagens de “e-mail marketing” oferecendo os produtos de quem pagar por estes serviços, mandar novas mensagens com outros “spywares” ou mesmo servir de base a partir do qual atacar servidores de empresas, tentando tirá-los do ar (os assim denominados ataques distribuídos de negação de serviços – “distributed denial of services”).

Trata-se de um problema antigo (ameaça de furto e divulgação de informações pessoais ou corporativas), sob uma roupagem contemporânea (possibilidade de interação direta do atacante com suas vítimas via correio eletrônico), cuja solução deveria atender, de um ponto de vista técnico, aos três pilares da Segurança de Informações:

- **Processos:** desenhar e implementar políticas, normas e procedimentos concernentes ao uso adequado dos sistemas corporativos de correio eletrônico e de acesso à Internet;
- **Pessoas:** desenvolver programas recorrentes de disseminação de boas práticas de uso de sistemas corporativos de correio eletrônico e de acesso à Internet;
- **Produtos:** implementar ferramentas de controle de sistemas corporativos de correio eletrônico e de acesso à Internet, que possam (i) evitar o recebimento de “spam”, (ii) evitar o recebimento de mensagens de correio eletrônico que contenham código hostil (“spywares”, vírus, worms e cavalos de tróia), (iii) evitar o acesso a “sites” da Internet conhecidos por disseminar “spywares” e outras chateações cibernéticas, (iv) evitar o “download” destas chateações cibernéticas, bem como (v) monitorar as estações de trabalho quanto a atividades de “spywares”, vírus, worms e cavalos de tróia.

Algumas fontes para informações adicionais:

APWG (Anti-Phishing Working Group). “What is Phishing and Pharming?” Disponível em www.antiphishing.org/index.html. Acesso em julho de 2005.

BARRACUDA NETWORKS. “Anti-Spyware Technology” Disponível em www.barracudanetworks.com/ns/products/anti_spyware_tech.php. Acesso em julho de 2005

CAMARGO, Francisco. “Depois do Phishing Scam, Vem aí o Pharming”. Disponível em www.clm.com.br/resourcecenter/docs/grupoclm/phishing.pdf. Acesso em agosto de 2005.

* Duval Costa, Administrador pela FGV, Mestrando em Segurança da Informação pelo IPT – USP é Diretor de Consultoria da ServNet Serviços Especializados.