A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

Nesta edição

Ataques de Phishing

EDITOR CONVIDADO

Pieter Danhieux é o editor convidado desta edição. Ele trabalha na BAE Systems Detica na Austrália (www.stratsec.net) e é instrutor do curso de teste de invasão no SANS Institute.

VISÃO GERAL

O email é uma das formas primárias da nossa comunicação. Nós não só o utilizamos diariamente para o trabalho, como também para manter contato com amigos e família. Além disso, o email é a forma pela qual empresas oferecem produtos e serviços como uma confirmação de compra online ou extratos bancários. Pelo fato de muitas pessoas ao redor do mundo dependerem do email, ele se tornou um dos métodos primários utilizados por criminosos cibernéticos para atacá-las. Nesta edição nós explicamos os perigos e os passos a tomar para proteger-se.

ATAQUES DE PHISHING

Phishing foi um termo utilizado originalmente para descrever um ataque desenvolvido para roubar dados de usuário e senha utilizados no acesso via Internet às contas bancárias. Entretanto o termo evoluiu e agora se refere a qualquer ataque baseado em email. Ele usa engenharia social, uma técnica onde o atacante tenta persuadi-lo a tomar uma ação. Frequentemente esses ataques começam com um email fingindo ser de alguém ou de uma fonte em que você confia, como um amigo, seu banco ou sua loja de Internet favorita. Esses emails então tentam seduzi-lo a tomar uma ação como clicar em um link, abrir um anexo ou responder uma mensagem. Os criminosos cibernéticos montam esses emails para parecerem convincentes, enviando-os a milhões de pessoas ao redor do mundo. Eles não têm um alvo específico em mente, nem sabem exatamente quem será sua vítima. Eles sabem apenas que quanto mais emails enviarem, mais pessoas poderão enganar. Ataques de phishing acontecem de quatro maneiras:

- **Colher Informações:** O objetivo do atacante é fazê-lo clicar em um link para levá-lo a um página de Internet que pedirá seu usuário e senha, ou talvez dados do seu cartão de crédito ou débito. Essas páginas de Internet podem parecer legítimas e ter exatamente a mesma aparência e funcionalidade do seu banco ou loja online, mas elas são páginas falsas desenvolvidas pelos atacantes cibernéticos para roubar suas informações;
- **Infectar seu computador com links maliciosos:** Mais uma vez o objetivo dos atacantes é fazê-lo clicar em um link. Entretanto, ao invés de colher suas informações,

Ataques de Phishing

querem infectar seu computador. Se você clica no link, você é direcionado a uma página de Internet que lança silenciosamente um ataque contra seu navegador de Internet e, se bem sucedido, dá acesso total ao seu computador, via Internet, para os atacantes cibernéticos;

- **Infectar seu computador com anexos maliciosos**: São emails de phishing que têm anexos maliciosos como arquivos PDF ou documentos Microsoft Office infectados. Se você abre esses anexos, eles atacam seu computador e, se bem sucedidos, dão ao atacante controle total ao seu computador;
- **Fraudes (Scam):** São tentativas dos criminosos para defraudá-lo. Exemplos clássicos incluem notícias de que ganhou na loteria (mesmo que nunca tenha jogado), pedidos de caridade logo após desastres recentes ou alguém que precisa transferir milhões de dólares para seu país e gostaria de pagá-lo para ajudar na transferência. Eles dizem então que você precisa pagar uma taxa inicial antes de enviar o dinheiro. Depois do seu pagamento, os criminosos desaparecem e não enviam mais mensagens.

PROTEGENDO-SE

Na maioria das vezes, abrir simplesmente o email é seguro. Para que o ataque funcione você tem que fazer alguma coisa depois de ler o email (como abrir o anexo, clicar em um link ou responder um pedido de informação). Aqui estão algumas indicações de que o email é um ataque:

- Suspeite de qualquer email que peça “ação imediata” ou crie um senso de urgência. Esse é um método comum utilizado para enganar as pessoas;
- Suspeite de emails endereçados a “Querido Cliente” ou qualquer outra saudação genérica. Se vier do seu banco, eles saberão seu nome;

Use bom senso. Se um email parecer único ou bom demais para ser verdade, é bem provável que seja um ataque.

- Suspeite de erros gramaticais ou de escrita. Muitas empresas fazem revisão gramatical em sua mensagens antes de enviá-las;
- Passe o mouse sobre o link. Isso mostrará o verdadeiro destino para onde será direcionado se clicar nele. Se o destino verdadeiro do link for diferente daquele escrito na mensagem, pode ser uma indicação de fraude;
- Não clique em links. Ao invés disso, copie a URL (endereço do link) do email que recebeu e cole no seu navegador de Internet. Melhor ainda, simplesmente digite esse endereço no seu navegador;
- Suspeite de anexos. Abra-os apenas quanto estiver esperando por eles;
- O fato de ter recebido email de um amigo não significa que ele o enviou. O computador do seu amigo pode ter

Ataques de Phishing

sido infectado ou sua conta de email pode ter sido comprometida e um malware (software malicioso) estar enviando o email para todos os contatos do seu amigo. Se você receber um email suspeito de um amigo ou colega em quem confia, ligue para ele para confirmar que, de fato, o enviou. Sempre ligue para o número de telefone que você já tem ou possa obter de forma independente e nunca para um número que venha na mensagem;

Se depois de ler um email você achar que é um ataque de phishing ou scam, simplesmente apague o email. Afinal, utilizar o email de forma segura é uma questão de bom senso. Se alguma coisa parecer suspeita ou boa demais para ser verdade, é bem provável que seja um ataque. Simplesmente apague o email.

RECURSOS

Alguns dos links abaixo foram abreviados para melhorar a leitura utilizando o serviço TinyURL. Para reduzir riscos de segurança, o OUCH! Sempre usa o recurso de pré visualização do TinyURL, que mostra o destino final do link e sempre pede sua permissão para prosseguir.

Anti-SPAM.br – Tipos de fraudes:
http://www.antispam.br/tipos/fraudes/

OnGuard Online (em Inglês):
http://www.onguardonline.gov/phishing

Anti-Phishing Working Group (em Inglês):
http://www.antiphishing.org

Reconhecendo Ataques de Phishing:
http://www.microsoft.com/pt-pt/security/online-privacy/phishing-symptoms.aspx

OpenDNS (em Inglês):
http://www.opendns.com/phishing-protection

Termos e Definições de Segurança:
http://cartilha.cert.br/glossario/

Security Terms & Definitions (em Inglês):
http://preview.tinyurl.com/6wkpae5

Delegacia de cyber crimes, por estado:
http://www.safernet.org.br/site/prevencao/orientacao/delegacias

SAIBA MAIS

Assine a publicação mensal OUCH! de sensibilização de segurança, acesse os arquivos OUCH! e aprenda mais sobre as soluções de sensibilização de segurança do SANS nos visitando em http://www.securingthehuman.org.

VERSÃO BRASILEIRA

Traduzida por:
Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Marcello Belloni Gomes, Arquiteto de Segurança de TI - twitter.com/marcellobelloni
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma

Time Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner