A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- O que é Engenharia Social
- Detectando / Parando os ataques de engenharia social

Engenharia Social

Visão geral

Uma ideia errada que a maioria das pessoas tem sobre os atacantes cibernéticos é de que eles usam apenas ferramentas e técnicas altamente avançadas para invadir computadores ou contas das pessoas. E isso não é verdade. Cyber atacantes aprenderam que muitas vezes as maneiras mais fáceis de roubar suas informações, entrar em suas contas ou infectar seus sistemas é simplesmente te enganando e levando você a cometer um erro. Neste boletim você aprenderá como esses ataques, chamados de engenharia social, funcionam e o que você pode fazer para se proteger.

Editor Convidado
James Lyne (**@jameslyne**) é instrutor SANS certificado e Chefe Global de Pesquisa da Sophos. Ele desfaz e aplica engenharia reversa nas maiores e mais recentes criações de criminosos cibernéticos. Ele também é autor dos cursos "Metasploit (SEC580)" e "Social Engineering (SEC567)", Engenharia Social, no SANS.

O que é Engenharia Social

A engenharia social é um ataque psicológico onde um invasor o engana levando você a fazer algo que não deveria fazer. O conceito de engenharia social não é novo, ele existe há milhares de anos. Pense em golpistas ou estelionatários, é a mesma ideia. O que torna a tecnologia de hoje muito mais eficaz para os atacantes cibernéticos é que você não pode vê-los fisicamente, eles podem facilmente fingir ser qualquer coisa ou alguém que eles querem e atingir milhões de pessoas em todo o mundo, incluindo você. Além disso, os ataques de engenharia social podem passar por muitas tecnologias de segurança. A maneira mais simples de entender como esses ataques funcionam e proteger-se deles é dar uma olhada em dois exemplos do mundo real.

Você recebe um telefonema de alguém que afirma ser de uma empresa de suporte a computadores, do seu Provedor de Internet ou talvez do Suporte Técnico da Microsoft. Quem ligou explica que seu computador está ativamente varrendo a Internet, e ele acredita que seu computador está infectado e foi encarregado de ajudá-lo a proteger seu computador. Em seguida, usa uma variedade de termos técnicos e o guia através de passos confusos para convencê-lo de que seu computador está infectado. Por exemplo, ele pode pedir-lhe para verificar se você tem certos arquivos em seu computador e orientá-lo sobre como encontrá-los. Quando você localizar esses arquivos, a pessoa que ligou garante que esses arquivos provam que seu computador está infectado, quando na realidade esses arquivos são arquivos de sistema comuns encontrados em quase todos os computadores do mundo. Depois de te enganar e você acreditar que seu computador está infectado, ele te leva a comprar um software de segurança dele ou a dar-lhe acesso remoto ao seu computador para que ele possa corrigi-lo. No entanto, o software que ele está vendendo é na realidade um programa malicioso. Se você comprar o software e instalá-lo, ele não só terá te enganado e infectado seu computador, como você o terá pago para isso. Se você

Engenharia Social

lhe der acesso remoto ao seu computador, ele vai assumir seu computador, roubar seus dados ou usá-los.

Outro exemplo é um ataque de e-mail chamado CEO Impostor, que acontece com mais frequência no trabalho. Ele acontece quando um cyber atacante pesquisa sua organização on-line e identifica o nome do seu chefe ou colega de trabalho. O atacante então faz um e-mail fingindo ser daquela pessoa e envia para o seu e-mail. O e-mail solicita urgentemente que você tome uma ação, como realizar uma transferência eletrônica ou enviar por e-mail informações confidenciais dos funcionários. Muitas vezes, esses e-mails fingem que há uma emergência que exige que você ignore os procedimentos de segurança padrão, por exemplo, eles podem pedir que você envie as informações altamente confidenciais para uma conta pessoal no gmail.com. O que torna os ataques direcionados como esses tão perigosos é que os atacantes cibernéticos fazem sua pesquisa antecipadamente. Além disso, as tecnologias de segurança, como antivírus ou firewalls, não conseguem detectar ou interromper esses ataques porque não há malware ou links maliciosos envolvidos.

O bom senso é a sua mais poderosa defesa para identificar e parar a maioria dos ataques de engenharia social.

Tenha em mente que os ataques de engenharia social como esses não se limitam a telefonemas ou e-mails; eles podem acontecer em qualquer forma, incluindo mensagens de texto em seu telefone, através de mídias sociais ou mesmo de uma pessoa. O essencial é saber que você é sua melhor defesa.

Detectando / Parando os Ataques de Engenharia Social

Felizmente parar tais ataques é mais simples do que você pode imaginar - o bom senso é a sua melhor defesa. Se algo lhe parece suspeito ou você não se sente confortável, pode ser um ataque. As pistas mais comuns de um ataque de engenharia social incluem:

- Alguém criando um tremendo senso de urgência, ele está tentando enganá-lo para que cometa um erro;
- Alguém solicitando informações que não deveriam ter acesso ou que já deveriam saber, como os números de sua conta;
- Alguém perguntando por sua senha. Nenhuma organização legítima jamais lhe pedirá isso;
- Alguém pressionando você para desconsiderar ou ignorar processos ou procedimentos de segurança que você deve seguir no trabalho;
- Algo muito bom para ser verdade. Por exemplo, você é notificado que ganhou a loteria ou um iPad, mesmo que você nunca tenha entrado na loteria;

Engenharia Social

- Você recebe um e-mail estranho de um amigo ou colega de trabalho, contendo expressões que não parecem vir deles. Um atacante cibernético pode ter invadido a conta dele e está tentando enganá-lo. Para se proteger, verifique essas solicitações, entrando em contato com seu amigo usando um método de comunicação diferente, como conversa pessoal ou por telefone.

Se você suspeitar que alguém está tentando enganar você, não se comunique mais com essa pessoa. Se o ataque estiver relacionado ao trabalho, não se esqueça de denunciá-lo imediatamente ao seu help desk ou à equipe de segurança da informação. Lembre-se, o bom senso é muitas vezes a sua melhor defesa.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Impostor:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser

