A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Sim, você realmente é um alvo

Visão Geral

Um erro comum de muitas pessoas é achar que não é um alvo do crime cibernético, que elas ou seus computadores não têm nenhum valor. Nada pode estar mais distante da verdade. Se você tem um computador, um dispositivo móvel, uma conta online, um endereço de e-mail, cartão de crédito ou se envolve em algum outro tipo de atividade online, você vale dinheiro para os criminosos cibernéticos. Nesta edição vamos explicar por que você é um alvo, como está sendo atacado e o que pode fazer para proteger-se.

Editor Convidado

Eric Conrad é presidente e CTO do Backshore Communications e autor líder dos livros "CISSP Study Guide", segunda edição e "Eleventh Hour CISSP", segunda edição. É também co-autor do curso SANS de seis dias "Continuous Monitoring and Security Operations (SEC511)".

Por que você é um alvo

Crimes como fraude, roubo de identidade ou extorsão existem desde os primórdios da civilização e são parte da nossa vida diária. O objetivo de um criminoso é sempre o mesmo: fazer o máximo de dinheiro possível, da forma mais fácil e com o menor risco possível. Tradicionalmente isto era difícil porque eles estavam frequentemente limitados à sua localidade e tinham que interagir fisicamente com suas vítimas. Isso não só limitava os possíveis alvos mas também expunha os criminosos a um alto risco. Contudo, o crime mudou radicalmente com o advento da Internet e a tecnologia disponível online. Agora os criminosos cibernéticos podem facilmente atacar qualquer pessoa ao redor do mundo, com baixo ou quase nenhum custo e com pouquíssimo risco. Adicionalmente, os criminosos cibernéticos têm se tornado altamente organizados e eficientes, fazendo com que sejam mais efetivos que nunca.

Hoje, os criminosos cibernéticos sabem que quanto mais cartões de crédito eles roubarem, quanto mais contas de banco hackearem ou mais senhas obtiverem, mais dinheiro eles podem fazer. Eles vão literalmente tentar hackear qualquer um conectado à Internet, inclusive você. Hackear milhões de pessoas ao redor do mundo pode parecer muito trabalho mas é surpreendentemente fácil ao se utilizar ferramentas automatizadas para fazer todo o trabalho para eles. Por exemplo, eles podem construir um banco de dados com milhões de endereços de e-mail e utilizar uma ferramenta automatizada para enviar uma mensagem de phishing para cada um desses endereços de e-mail. Enviar os e-mails custa para os criminosos praticamente nada: eles simplesmente utilizam outros computadores hackeados, talvez até o seu, para fazer o trabalho sujo deles. Este é também mais um exemplo de por que seus aparelhos têm valor, eles podem utilizá-lo para hackear ou prejudicar os outros. Em última análise os criminosos não sabem

Sim, você realmente é um alvo

quem serão as vítimas dos seus ataques de e-mail mas eles sabem que quanto mais e-mails enviarem, mais pessoas eventualmente se tornarão vítimas. Ou talvez os criminosos possam literalmente varrer cada computador na Internet (mais uma vez utilizando computadores hackeados para fazer a varredura), procurando por outros computadores ou dispositivos que possam hackear. Lembre-se, você não está sendo escolhido por que é especial. Esses criminosos estão mirando todos que puderem, o que passa a incluir você.

Você pode não perceber mas seus dispositivos e suas informações pessoais têm um tremendo valor para criminosos cibernéticos ao redor do mundo.

Protegendo-se

Quando os criminosos cibernéticos tentam hackear pessoas ao redor do mundo, eles estão tipicamente utilizando métodos relativamente simples. Felizmente, ao seguir passos igualmente simples você dá uma boa sobrevida à sua segurança. Alguns dos passos que recomendamos incluem os seguintes:

- **Você mesmo**: em última análise, você é a primeira linha de defesa de qualquer atacante cibernético. Muitos ataques começam com um criminoso cibernético tentando enganá-lo, como tentando fazê-lo abrir um anexo infectado de um e-mail ou fazendo-o informar sua senha pelo telefone. Bom senso é a sua melhor defesa: se algo parece estranho, suspeito ou muito bom para ser verdade, provavelmente é um ataque;

- **Atualizações**: Certifique-se que qualquer computador ou dispositivo móvel que você utiliza esteja totalmente atualizado e tenha todas as últimas correções. Não apenas o sistema operacional mas qualquer aplicativo ou plugin que esteja utilizando. Ao manter seus sistemas e aplicativos sempre atualizados você ajuda a proteger-se dos ataques mais comuns;

- **Senhas**: Use uma senha única e forte para cada uma de suas contas. Assim quando um site de Internet que você usa for hackeado e tiver todas as senhas comprometidas (inclusive a sua), as suas outras senhas estarão protegidas. Certifique-se também que todos os seus outros dispositivos estão protegidos por uma senha única e forte, por um PIN ou outro tipo de mecanismo de trava. Para manter um controle seguro de todas as suas diferentes senhas nós recomendamos que utilize um Gerenciador de Senhas;

- **Cartões de Crédito**: Verifique seus extratos frequentemente – nós recomendamos pelo menos uma vez por semana (uma vez por mês não é suficiente). Tão logo perceba uma transação não autorizada, relate imediatamente para a administradora do cartão. Se seu banco disponibiliza serviços de alerta por e-mail

Sim, você realmente é um alvo

ou torpedos no celular (SMS) para transações incomuns ou muito grandes, utilize-os para notificações mais rápidas sobre atividades suspeitas;

- **Sua Rede**: Utilize uma senha forte para o usuário Administrador do ponto de acesso Wi-Fi da sua rede pessoal e certifique-se que sua rede Wi-Fi solicita uma senha a quem tentar utilizá-la. Além disso identifique os dispositivos que estão conectados à sua rede pessoal e certifique-se de que todos estão atualizados.

- **Midia Social**: Quanto mais informação você publica online, mais provavelmente você se expõe a riscos. Essas informações não somente tornam você um alvo mais fácil para que os criminosos cibernéticos o enganem, mas também podem identificá-lo como um alvo mais valioso;

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 http://www.securingthehuman.org.

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
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

OUCH! Gerenciadores de Senha:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Protegendo Sua Rede Doméstica (de casa):	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Ataques de Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: Você é O Alvo:	http://www.securingthehuman.org/resources/posters

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser