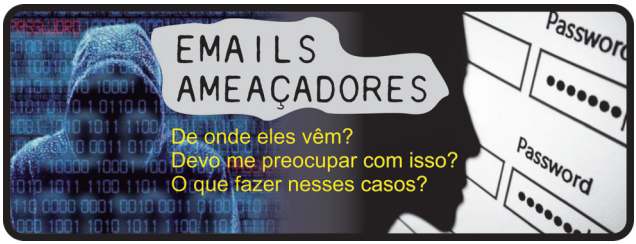

Muita gente recebe mensagens, geralmente em inglês, ameaçando postar vídeos de seus momentos mais íntimos na internet, entre outras ameaças. Isto só não será feito se a pessoa depositar determinada quantia em Bitcoins (ou outra moeda virtual) numa determinada conta. De onde vêm estas mensagens? Devo me preocupar com isso? O que fazer? Como nos proteger?

À primeira vista essas mensagens são bastante verossímeis. Elas parecem incluir informações secretas sobre o destinatário que nos leva a crer que as ameaças são reais. Em especial, elas informam alguma senha efetivamente usada pelo dono daquele email.

Aliás, estas mensagens sempre começam com a parte mais convincente do email: a afirmação de que a pessoa que o envia tem sua senha, que geralmente consta na própria mensagem. Na maioria delas o remetente que aparece é o próprio email do destinatário, dando a entender que o invasor tem a senha e pode enviar emails usando a conta que foi invadida.

Depois desta apresentação, começa com uma série de ameaças e termina pedindo um resgate. "Vou direto ao ponto", diz uma dessas mensagens. "Você não sabe nada sobre mim, enquanto eu agora sei muito sobre você e agora você provavelmente está pensando por que você está recebendo este email, certo?"

Prossegue afirmando que o remetente foi capaz de invadir o computador ou celular e instalar ali um tipo de malware capaz de assumir o controle da webcam e também de gravar as imagens da tela. Alega que, com isso, conseguiu gravar vídeos do destinatário enquanto ele via pornografia. Explica que este mesmo malware não é detectado pelos antivírus, e que mesmo que seja removido ele vai se reinstalar. Também avisa que não adianta trocar a senha do email, porque agora que o malware está instalado ele vai detectar a mudança da senha e avisar o remetente.

Depois de explicada a situação, o email faz a ameaça: se a pessoa que recebe a mensagem não pagar uma certa quantia em Bitcoins (algo entre $400 a $900, sem especificar a moeda) então esses vídeos comprometedores serão enviados para a família do usuário e para todos seus contatos.

Se você recebeu uma mensagem assim, a primeira coisa é ter calma. A maioria delas é falsa, e mesmo que fossem verdadeiras, ainda há muita coisa por fazer antes de mandar dinheiro para o malandro.

Quem é que manda estas mensagens?

Em geral essas mensagens são uma farsa, uma ameaça vazia, tentando tirar proveito de um momento de fraqueza das pessoas.

Várias partes da mensagem sinalizam que ela é uma farsa. Por exemplo, o tal meliante alega ter gasto muito tempo observando o destinatário do email, mas ele não fornece qualquer detalhe sobre o que eles têm. Nem sequer uma foto com o rosto do dono da conta de email ou um email de algum contato seu.

Os remetentes procuram compensar esta falha pelo fato de a mensagem incluir uma senha, sugerindo que realmente houve algum tipo de violação. Isso pode ter acontecido, mas via de regra essas senhas são antigas, coisa de 10 ou mais anos, e podem ter sido conseguidas no vasto repertório de senhas roubadas que estão disponíveis nos sites de hackers.

Essas senhas podem ter vindo de um dos vazamentos de dados dos usuários que atingiram grandes empresas nos últimos anos. Muitos dos maiores ser-