UTILIDADE PÚBLICA
Amigos, recebi um e-mail numa conta praticamente desativada dizendo ser hacker vietnamita que invadiu meu computador e exigindo pagamento em bitcoins. Isso procede?Pode acontecer?

Isso procede?Pode acontecer?
Pode proceder/acontecer. Tenho recebido questionamentos como este que se mostraram verídicos depois.

um e-mail
Isso pode ser interessante para comprovar a origem da mensagem. Em geral, as mensagens de eMail carregam uma longa trilha do caminho que ele teve que percorrer até chegar em você.
Alem disso, contem informações sobre o ambiente (sistema operacional, aplicativo de e-mail, configurações de rede etc).
Providencias: Preservar a mensagem para perícias.

um e-mail numa conta praticamente desativada
Isso é um tanto suspeito! Pode indicar que ele coletou em algum momento e tenta usar agora.
A coleta de endereços de e-mail pode ser feita de diversas formas, mas uma das mais comuns é a observação da sua participação em blogs, foruns, comentários, entre outros.
Dúvida: Este e-mail (praticamente desativado) foi usado em algum lugar? Conseguimos recuperar isso?

Dizendo que invadiu o meu computador.
Estranho. O normal é ele mostrar os "estragos" de forma que você (vítima) já tenha percebido "algo estranho". Por exemplo, alguns arquivos não abrem como acontecia normalmente, ou a máquina começa a demonstrar comportamento "diferente".
Sem que você tenha percebido nada de diferente, ainda é possível que ele esteja tentando fazer você se mexer de alguma forma (clique, resposta ao e-mail, etc) para tirar proveito.
Mas, "invadiu" é um tanto genérico.

exigindo pagamento em bitcoins
Essa forma de pagamento se tornou bem comum nestes casos justamente pela falta de rastreabilidade.

Providencias
Fake News – Não levaria a ameaça tão despreocupadamente. Os estragos em casos reais de invasão são grandes, em especial em casos em que a vida profissional tem base no mundo digital. Cabem avaliações antes de descartar a ameaça como Fake News. Infelizmente, estamos vivendo a Fábula do Pedro e o Lobo.

E-Mail – Procurar rastrear a grande evidencia que temos da ameaça. Em geral, um malfeitor deixa pistas, mesmo que ele tente escondê-las.

Quarentena. - Pode ser de grande desconforto, mas cabe considerar uma quarentena para os seus equipamentos.

Cópias Backup e Verificações de ambiente. Se a ameaça ainda estiver em curso, retirar do ambiente em uso os objetos de valor (documentos, fotos, contratos, etc) é uma providência razoável! Verificar o ambiente (configurações, usuários, logs, etc) na busca de evidencias. Em geral, se deixa rastros, ou mesmo marcas de que os rastros foram apagados.

Rescan com Antivírus e outros produtos de segurança. Em geral, os produtos de segurança recomendam procedimentos específicos para incidentes. Cabe seguir as instruções do seu fornecedor predileto. *Quis custodiet ipsos custodes?*

Procedimentos de Segurança. É uma boa oportunidade para a revisão (paranoica) dos procedimentos de segurança.

Resgate. A minha politica geral continua sendo “Não pago resgate”! Mas o mercado está migrando para “pode ser uma alternativa a se considerar”!