Dois golpe utilizando WhatsApp. Leia sobre eles a seguir

Brecha no WhatsApp permite entrar em grupos e ler mensagens sem autorização[1]

Há dois anos o WhatsApp incluiu em seu serviço de mensagem a criptografia de ponta-a-ponta, prometendo manter seguras as conversas dos seus usuários. No entanto, conforme relata o site Wired, parece que o sistema de segurando do aplicativo possui falhas que permitem a espionagem das conversas.

Um grupo de pesquisadores da Universidade Ruhr apresentou, dia 10/01, durante uma conferência de segurança do Real World Crypto uma série de falhas em aplicativos de mensagens que dizem ter criptografia, entre eles o WhatsApp, Signal e Threema.

O estudo mostra que, apesar de muitos aplicativos apresentarem falhas relativamente inofensivas, foram encontradas brechas graves no WhatsApp. Uma pessoa que controle os servidores do WhatsApp, como funcionários ou membros do governo, poderia adicionar uma pessoa em um grupo de conversa, de forma privada, sem a autorização do administrador – permitindo assim o acesso a todas as mensagens enviadas.

Apesar de se tratar de uma brecha quase impossível de ser explorada pelo cibercrime, já que depende do controle dos servidores do aplicativo, a vulnerabilidade afeta uma relação de confiança criada com a introdução da criptografia de ponta-a-ponta. Com a tecnologia, o WhatsApp prometeu que seria impossível para a empresa, para autoridades ou para hackers interceptar mensagens que circulam pelo app. No entanto, um funcionário "engraçadinho" poderia entrar em algum grupo sem autorização e ler o que é publicado, e as autoridades também poderiam emitir um mandado que obrigue a empresa a dar acesso a um grupo, permitindo descobrir tudo que se conversa naquele espaço.

Os pesquisadores afirmam que a brecha aproveita um erro simples: somente o administrador de um grupo pode convidar novos membros, mas o WhatsApp não usa nenhum mecanismo de autenticação para esse convite. Isso significa que é possível adicionar novos membros a partir dos servidores do Whatsapp, sem precisar interagir com o administrador.

Um porta-voz do WhatsApp confirmou a descoberta, mas diz que a empresa não pretende lançar uma correção. A justificativa é justamente a dificuldade de explorar a brecha, especialmente porque quando alguém entra em um grupo, o aplicativo exibe um alerta de que há um novo participante na conversa. De fato, em grupos pequenos, como o da sua família, dificilmente um invasor passaria despercebido; no entanto, se

[1] Juliana Américo 10/01/2018 criptografia Segurança Whatsapp

pensarmos em grupos maiores, ficaria praticamente impossível perceber que alguém entrou sem autorização.

Então para aqueles usuários compulsivos, controlem-se.

Golpe do falso processo seletivo via WhatsApp atinge 1 milhão de pessoas[2]

Os cibercriminosos estão se aproveitando da alta do desemprego entre os brasileiros para espalhar golpes. De acordo com o DFNDR Lab, da PSafe, mais de 1 milhão de pessoas caíram em um golpe que está circulando pelo Whatsapp e que divulga um falso processo seletivo para trabalhar em uma rede de supermercados atacadista.

O usuário recebe uma mensagem que promete a participação em um processo seletivo com salários de até R$ 2.800, além de benefícios, como assistência média, vale-refeição, vale-transporte e seguro de vida, e que para participar, a pessoa precisa acessar um link e responder três perguntas.

Ao entrar clicar no link e responder as perguntas, a vítima é encaminhada para uma nova página que contém uma mensagem perguntando se ela gostaria de agendar uma entrevista. Ao clicar na opção "Sim, claro", a pessoa acaba autorizando o hacker a enviar notificações de outros golpes por push. A página ainda solicita o compartilhamento da oportunidade com todos os contatos e grupos do WhatsApp.

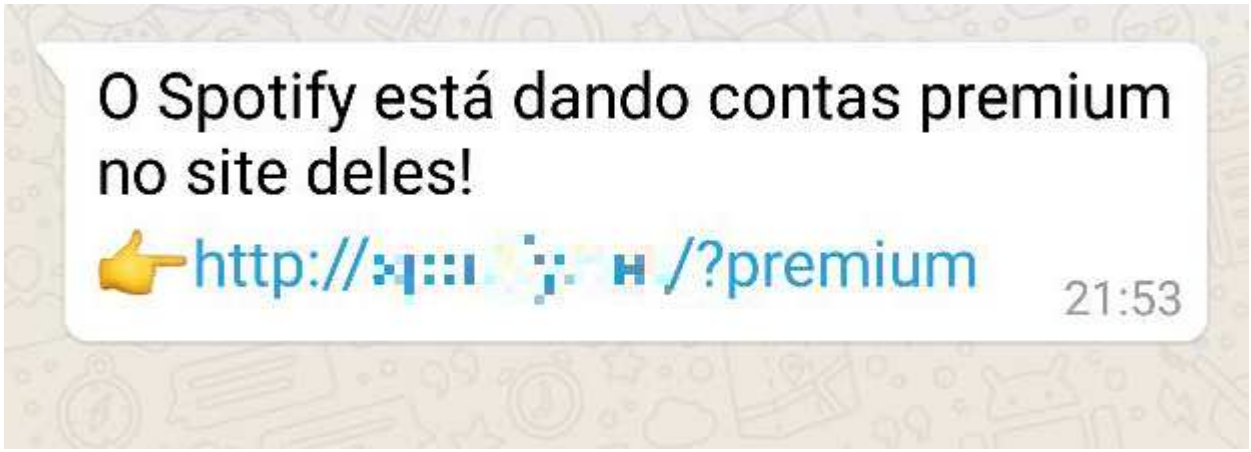
Para evitar cair nesse tipo de golpe, a orientação é de que os internautas não abram links suspeitos, mesmo quando enviados por pessoas conhecidas, e desconfiem de promoções e oportunidades muito vantajosas, além de erros gramaticais. No caso de mensagens ligadas às empresas, verifique no site e redes sociais da mesma se a promoção ou seleção de emprego são verdadeiras.

[2] Juliana Américo 12/01/2018 ciberataque cibercrime Crimes digitais

Golpe no WhatsApp promete Spotify grátis e sem anúncios; veja como evitar

Fique de olho no que você recebe e compartilha pelo WhatsApp. O aplicativo tem sido veículo de mais um dos golpes que visam enganar sua enorme base de usuários a fim de infectar aparelhos ou roubar dados privativos. A bola da vez é a promessa de contas premium grátis do Spotify.

A corrente em questão vem com um link falso para o site do Spotify, que não citaremos aqui para não levar mais visitantes à página. A URL, porém, traz o nome da empresa escrito errado e ainda por cima usa um domínio ".net" em vez do ".com" usado pelo serviço real.



Esse tipo de golpe já é clássico. Usuários são atraídos com a promessa de cupons de descontos ou produtos grátis, mas ao acessar a página, que imita o site verdadeiro, a vítima é orientada a fornecer informações pessoais e às vezes até mesmo dados de cartão de crédito. Além disso, para o golpe se espalhar, o site também determina que a vítima deve enviar a mensagem para um número específico de grupos ou contatos para ter acesso ao suposto benefício.

Neste caso específico, o site exibe algumas perguntas inofensivas antes de pedir que a vítima compartilhe a página com seus contatos. A tacada final vem em seguida, quando o usuário pressiona o botão "Ativar conta". Para completar, a página replica uma seção

de comentários do Facebook com várias pessoas comentando positivamente sobre a promoção, quando na verdade é algo que apenas parece com o recurso do Facebook, sem ser, de fato, uma área de comentários funcional.

Em contato com o Olhar Digital, a empresa de segurança digital ESET comentou que esse tipo ataque tem se popularizado. "O Whatsapp tem se tornado uma popular ferramenta para tentativas de phishing (ataques geralmente enviados por meio de aplicativos de mensagens e disfarçados em forma de produtos grátis ou cupons promocionais que, para serem acessados, exigem o preenchimento de cadastro com dados como número do cartão de crédito, senhas e outros). Para atrair ainda mais a atenção das possíveis vítimas, os fraudadores escolhem empresas renomadas como o Spotify, o Burger King, Netflix, entre outras, para disfarçar o golpe. ***A ESET orienta os usuários a desconfiar de mensagens que ofereçam promoções que pareçam muito boas para ser verdade, e nunca preencher dados pessoais, números de documentos e cartões em links suspeitos fornecidos fora dos sites oficiais das empresas. Em caso de dúvidas, consulte os sites oficiais da empresa", diz o comunicado.***