Vytautas Zumas: Fleeceware: quem nunca?

É notória a influência e a infiltração de novas tecnologias em nosso cotidiano. Nossos telefones celulares, hoje chamados de *smartphones*, tornaram-se agendas, computadores, *streamers* de áudio e

e ainda fazem ligações telefônicas!

A magnitude de possibilidades só é possível ante a infinidade de aplicativos disponíveis para os sistemas operacionais de cada dispositivo. As conhecidas lojas virtuais fornecem uma infinidade de *softwares* e representam verdadeiro repositório de praticidades, lazer, entretenimento e produtividade.

No entanto, a alta circulação de usuários nessas *stores* obviamente chama a atenção daqueles comprometidos em obter vantagem financeira indevida. Uma rápida pesquisa nas duas mais populares lojas virtuais permite a verificação de milhares de aplicativos das mais diversas modalidades com bilhões de *downloads* anuais. Obviamente a pandemia causada pelo coronavírus e o decorrente isolamento social fizeram com que a quantidade de *downloads* aumentasse ainda mais.

É fato que as lojas oficiais são lugar mais seguro para a obtenção de aplicativos não maliciosos. Porém, todo esforço para a proteção da segurança cibernética dos usuários não significa que estaremos imunes a qualquer tipo de lesão.

Se por um lado criminosos dificilmente conseguem infiltrar aplicativos com códigos maliciosos nas lojas oficiais, podem muito bem obter vantagens com aplicativos que não possuem nenhuma ameaça em seu código-fonte, cumprem o que prometem, mas possuem cobranças recorrentes abusivas. Trata-se de modalidade de golpe chamada *fleeceware.* O substantivo atribuído ao golpe foi cunhado pela empresa americana Sophos e vem do verbo inglês *to fleece*, que significa levar o dinheiro de alguém de forma desonesta, cobrando muito dinheiro ou enganando-o.

E é exatamente o que alguns aplicativos existentes nas lojas oficiais fazem. Uma lanterna que cobra nove dólares por semana ou um aplicativo de filtros para fotos que cobra 35 dólares por mês são claros exemplos desse tipo de manobra. Os desenvolvedores de tais aplicativos aproveitam-se de modelo de negócio em que o usuário pode fazer uso da aplicação por curto período de tempo gratuitamente (usualmente apenas três dias). Transcorrido tal lapso temporal sem que o usuário o tenha desinstalado ou cancelado a assinatura, o aplicativo efetua cobranças na conta do usuário por meio do cartão de crédito

2023 - www.conjur.com.br - Todos os direitos reservados.

pré-cadastrado.

Como os aplicativos não possuem nenhum código malicioso, as lojas oficiais não os vetam de imediato e apenas com as denúncias feitas pelos usuários lesados as plataformas podem tomar alguma atitude. Por isso é muito importante que, antes de baixar um aplicativo desconhecido, o usuário leia as avaliações (principalmente as ruins), pois assim poderá ter certeza de que não estará sendo vítima de *fleeceware*.

Outra forma de proteção é manter no dispositivo apenas a quantidade mínima necessária de aplicativos, possibilitando assim melhor controle daquilo que está armazenado e nunca abrir links ofertados em anúncios, mesmo que no ambiente de outros aplicativos. Caso deseje baixar algum aplicativo, digite diretamente na *app store* e verifique se não há outros com ícones e nomes similares. O uso de soluções de confiança como antivírus desenvolvidas para o sistema operacional de seu telefone também é uma boa opção.

Caso já tenha sido lesado, estes passos ajudarão no cancelamento da assinatura: no sistema operacional iOS, acesse "Ajustes", toque no seu nome e foto na parte superior da tela e, em seguida, toque em "Assinaturas" para visualizar e gerenciar tudo. Importante também deixar a função de "Recibos de Renovação" sempre ativada, assim você receberá o recibo a cada cobrança pelo aplicativos contratados. Também é possível abrir a *App Store*, tocar nas suas iniciais ou foto no canto superior direito e tocar em "Assinaturas". No Android, abra a *Play Store*, toque no ícone com três linhas horizontais no canto superior direito e escolha "Assinaturas" para visualizar e gerenciar suas inscrições.

No Brasil, tal prática é vedada pelo Código de Defesa do Consumidor (artigos 39 e 51) e a conduta pode ser tipificada como crime previsto no artigo 66 do mesmo diploma, com pena de detenção de três meses a um ano e multa.

Date Created
12/06/2020

2023 - www.conjur.com.br - Todos os direitos reservados.