A TRIBUNA
Publicado em 01/02/2023 - 05:51

Novo golpe com cartão por aproximação utiliza vírus

Vírus Prilex gera fraude com cartão de aproximação

Empresa alerta para mensagem falsa de erro

ADOBE STOCK

Nas lojas, computador usado para pagamento não pode ter outro fim, enquanto consumidor não deve usar cartão físico se frase de erro surgir

DE SÃO PAULO

A empresa de cibersegurança Kaspersky anunciou que descobriu variações do vírus brasileiro Prilex, e que o malware (programa malicioso) agora é capaz de bloquear pagamentos por aproximação de cartão. Após uma mensagem de erro, o consumidor é obrigado a inserir o cartão na maquininha, o que possibilita que o malware roube dados e fraude transações.

O golpe bloqueia pagamentos que utilizam a tecnologia NFC, que teve crescimento durante a pandemia e possui um mecanismo de segurança que cria um número de cartão único para cada transação - as informações, mesmo que capturadas por criminosos, não teriam utilidade.

Quando há dispositivos infectados no ponto de venda, porém, a operação será bloqueada e uma falsa mensagem de erro irá aparecer: "Erro aproximacao insira o cartao (sic)".

O objetivo é obrigar o consumidor a inserir o cartão na maquininha, momento em que o malware captura os dados da transação, incluindo o número do cartão físico, tornando-o vulnerável a transações indevidas.

Segundo a Kaspersky, o Prilex é o primeiro malware capaz de realizar fraudes com esse tipo de tecnologia de pagamento, mesmo que de forma indireta.

O malware ainda é capaz de filtrar cartões de crédito de acordo com o segmento, podendo, por exemplo, bloquear somente as operações de cartões black, corporativo ou outras opções que costumam ter limites mais altos.

O Prilex é um grupo brasileiro especializado em fraudes financeiras. Sua atuação é rastreada desde 2014 na América Latina e já foi identificada também na Europa. Por enquanto, as novas versões do vírus foram detectadas somente no Brasil, mas poderão ser disseminadas para outros países, segundo a Kaspersky.

COMO SE PROTEGER

Como as ferramentas do Prilex afetam computadores de pontos de venda, é preciso que os lojistas se atentem à segurança de suas operações. Computadores usados para sistemas de pagamento não devem ser utilizados para outros fins, e é necessário que o sistema tenha uma solução de segurança atualizada e robusta, de preferência soluções com várias camadas de proteção. Equipamentos com sistemas antigos também devem ter soluções de segurança otimizadas para suas versões.

Já os consumidores devem ficar atentos à falsa mensagem de erro: caso ela apareça, o usuário não deve recorrer ao cartão físico, mas a outros meios de pagamento, como dinheiro ou Pix. É importante acompanhar os valores emitidos na fatura do cartão e na conta corrente.

Se for detectado algum gasto indevido, é preciso entrar em contato com a instituição financeira para tentar uma solução. Também é recomendável fazer boletim de ocorrência. (Estadão Conteúdo)

Veículo: Impresso -> Jornal -> Jornal A Tribuna - Santos/SP

Seção: Economia **Caderno:** B **Pagina:** 1

Copyright © Clipclap 2025.