Quarta-Feira, 11 de Fevereiro de 2026

Vírus que assume controle do WhatsApp rouba senhas e tira print da tela; entenda

Segundo a empresa Karpersky, responsável pelos bloqueios, **o golpe começa quando o usuário recebe um arquivo compactado (.zip)** pelo WhatsApp contendo um arquivo de atalho (.LNK) malicioso. As investigações indicam que o "novo trojan" compartilha código e técnicas com o Coyote — trojan brasileiro identificado em 2024.

"Essas semelhanças sugerem que o maverick pode ser uma evolução ou um projeto paralelo dos mesmos desenvolvedores do Coyote", analisa a Karpersky.

Conforme a empresa, ao abrir o arquivo, **a ameaça verifica se a vítima está no Brasil** — com análise de fuso horário, idioma e formato de data e hora do computador — e só dá continuidade ao trabalho se detectar que as configurações são brasileiras. Ele também não funciona em celulares: mira computadores.

Uma vez confirmada a nacionalidade, o malware inicia uma **cadeia de infecção complexa que ocorre totalmente na memória do computador**, dificultando sua detecção.

"O que mais chama a atenção no maverick é sua sofisticação e sua ligação com ameaças anteriores. Ele compartilha partes importantes do código com o Coyote, um trojan que descobrimos em 2024, o que sugere que os criminosos estão evoluindo e reescrevendo seus componentes para torná-los mais perigosos. Além disso, a capacidade de se espalhar automaticamente pelo WhatsApp o torna um worm com potencial de crescimento exponencial, elevando o impacto do golpe. É uma das cadeias de infecção mais complexas que já vimos para um trojan bancário", comenta Anderson Leite, analista de segurança da Karpersky.

Como age o vírus?

Depois que consegue infectar o computador da vítima, o vírus tenta acessar um dos 26 bancos brasileiros ou as seis corretoras de criptomoedas monitoradas por ele — não foram ditas pela pesquisa quais são as instituições financeiras.

De acordo com especialistas, a ameaça é capaz de controlar totalmente o dispositivo, além de tirar capturas de tela, monitorar acesso a sites, registrar o que é digitado e até mesmo utilizar a conta de WhatsApp da vítima para se espalhar para contatos dela, automatizando o envio de mensagens fraudulentas.