Como o WhatsApp Web virou porta de entrada para ataque hacker com foco no Brasil

Foto:Reprodução | Batizado de Sorvepotel, vírus identificado pela Trend Micro usa o aplicativo de mensagens para se infiltrar em computadores com Windows e tem o Brasil como destino de quase todas as infecções registradas.

Baixar arquivos suspeitos no WhatsApp Web pode abrir caminho para criminosos assumirem o controle de computadores e roubarem senhas, informaram pesquisadores da empresa de cibersegurança Trend Micro.

O vírus, batizado de Sorvepotel, se espalha por meio de arquivos enviados em conversas e grupos de WhatsApp e usam e-mails como uma segunda forma de se espalhar. Caso sejam executados na máquina da vítima, eles se infiltram no computador de forma persistente.

“É aberta uma porta de comunicação e, a partir disso, o sistema de ataque passa a receber instruções externas”, explica Marcelo Sanches, líder técnico da Trend Micro Brasil. “A máquina da vítima fica sob comando do atacante”.

Como o vírus só funciona em computadores com Windows, os cibercriminosos enviam mensagens como “Baixa o ZIP no PC e abre” acompanhadas de comprovantes de pagamento e orçamentos falsos.

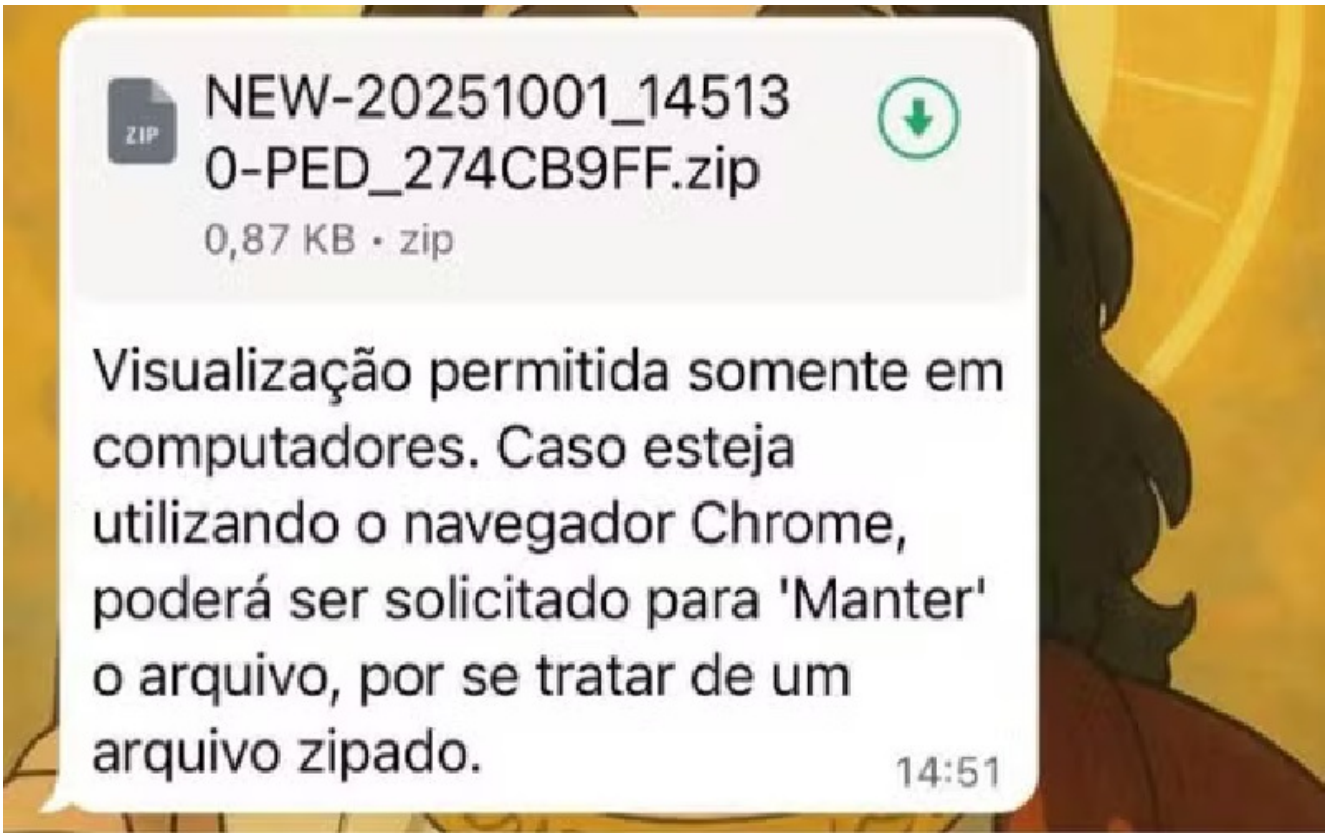
Segundo a Trend Micro, o ataque se concentra em:

roubar credenciais ao exibir versões adulteradas de sites de bancos e corretoras de criptomoedas;
assumir o controle do WhatsApp Web para enviar o mesmo arquivo malicioso para todos os contatos da vítima.

De acordo com a Trend Micro, 457 das 477 infecções registradas até agora ocorreram no Brasil.

Os pesquisadores apontaram o foco no país porque o arquivo faz checagens de idiomas, localização, formato de data para validar que o usuário é brasileiro.

O WhatsApp orienta usuários a clicarem apenas em links ou arquivos de pessoas conhecidas e diz que trabalha para tornar o aplicativo mais seguro (leia a nota ao final).



Mensagem no WhatsApp induz vítima a baixar vírus — Foto: Reprodução/Trend Micro

Até mesmo o nome Sorvepotel indica o direcionamento para o Brasil: os servidores usados pelo vírus para enviar comandos de ataques estão em endereços que lembram a expressão “sorvete no pote”.

Em computadores infectados, o malware também cria um arquivo

de inicialização, garantindo que o sistema malicioso continue ativo mesmo após reiniciar a máquina.

Ainda não há registros expressivos de roubo de dados ou bloqueio de arquivos, indicando que o objetivo neste momento é se espalhar para novos dispositivos, segundo a Trend Micro.

O ataque também pode fazer com que a conta da vítima seja banida do WhatsApp, já que o envio automático de mensagens para outros contatos pode ser identificado como spam.

Como se proteger

Os pesquisadores afirmam que criminosos parecem ter como foco computadores corporativos, mas atacam em contas de WhatsApp Web de funcionários, que usam os dispositivos para ver mensagens pessoais.

O vírus não explora falhas do WhatsApp, mas aproveita a distração das vítimas, diz Marcelo Sanches, da Trend Micro. Segundo ele, a ação permite transformar a máquina em um "zumbi" sob controle dos hackers.

Os pesquisadores da Trend Micro orientam usuários e empresas a:

desativar downloads automáticos no WhatsApp
restringir downloads em dispositivos corporativos
realizar treinamentos sobre riscos de baixar arquivos suspeitos;
desconfiar de mensagens que pedem permissões em navegadores;
confirmar com a pessoa por outros meios (telefone ou pessoalmente) se o envio do arquivo foi intencional.

Leia a nota do WhatsApp:

"Independentemente do serviço de mensagens que você use, só clique em links ou abra arquivos de pessoas que você conhece e confia. Estamos sempre trabalhando para tornar o WhatsApp o lugar mais seguro para a comunicação privada, e é por isso que

criamos camadas de proteção que oferecem mais contexto sobre com quem você está conversando ao receber uma mensagem de alguém que você não conhece – além de proteger suas conversas pessoais com a criptografia de ponta a ponta.”

Fonte: NBC News e Publicado Por: Jornal Folha do Progresso em 13/10/2025/10:29:24

O formato de distribuição de notícias do Jornal Folha do Progresso pelo celular mudou. A partir de agora, as notícias chegarão diretamente pelo formato Comunidades, ou pelo canal uma das inovações lançadas pelo WhatsApp. Não é preciso ser assinante para receber o serviço. Assim, o internauta pode ter, na palma da mão, matérias verificadas e com credibilidade. Para passar a receber as notícias do Jornal Folha do Progresso, clique nos links abaixo siga nossas redes sociais:

- **Clique aqui e nos siga no X**
- **Clica aqui e siga nosso Instagram**
- **Clique aqui e siga nossa página no Facebook**
- **Clique aqui e acesse o nosso canal no WhatsApp**
- **Clique aqui e acesse a comunidade do Jornal Folha do Progresso**

Apenas os administradores do grupo poderão mandar mensagens e saber quem são os integrantes da comunidade. Dessa forma, evitamos qualquer tipo de interação indevida. Sugestão de pauta enviar no e-mail:folhadoprogresso.jornal@gmail.com.

Envie vídeos, fotos e sugestões de pauta para a redação do JFP (JORNAL FOLHA DO PROGRESSO) Telefones: WhatsApp (93) 98404 6835– (93) 98117 7649.
“Informação publicada é informação pública. Porém, para chegar

até você, um grupo de pessoas trabalhou para isso. Seja ético. Copiou? Informe a fonte.”

Publicado por Jornal Folha do Progresso, Fone para contato 93 981177649 (Tim) WhatsApp:-93- 984046835 (Claro) -Site: www.folhadoprogresso.com.br e-mail:folhadoprogresso.jornal@gmail.com/ou e-mail: adeciopiran.blog@gmail.com