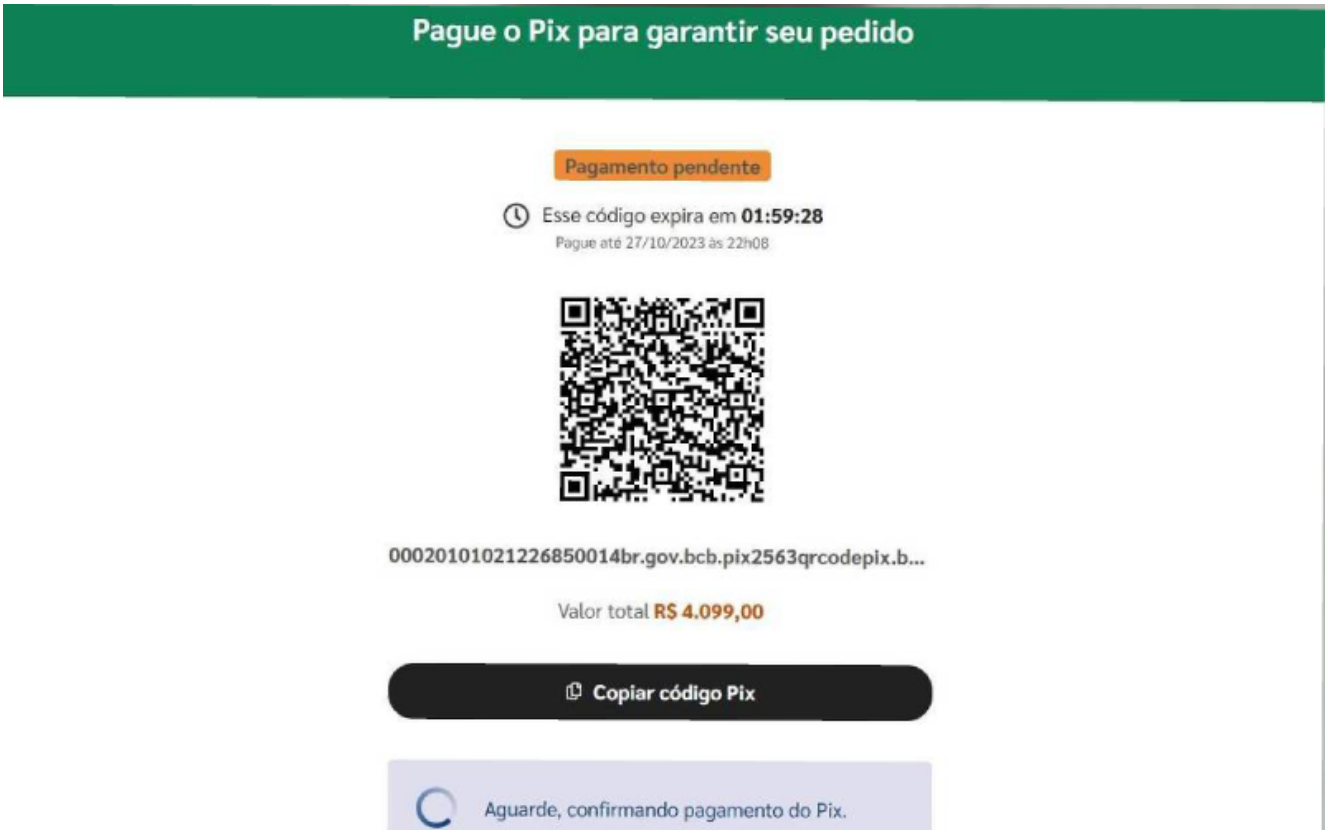
Quadrilha usa vírus de computador para desviar Pix e pagamentos com cripto e boleto

Category: BRASIL,GERAL,TECNOLOGIA e CIÊNCIA
escrito por Chellsen Carneiro | 17 de março de 2026

Um vírus de computador que frauda compras online alterando o destino da transferência ganhou novas funções. Agora, além do Pix, o chamado GoPix desvia pagamento de boleto e operações com criptomoedas.

Segundo relatório do antivírus Kaspersky divulgado nesta segunda-feira (16), esse programa malicioso explora uma ferramenta legítima do navegador para redirecionar sites —o objetivo é mudar o destinatário da transferência e fazer mudanças sutis na chave Pix, no código do boleto ou na senha criptográfica da criptomoeda.

Com isso, não ficam pistas do golpe no computador, dificultando a detecção do vírus. “Esse trojan bancário brasileiro se consolida como a ciberameaça financeira mais avançada do país”, diz o relatório da empresa. A Kaspersky não consegue rastrear o tamanho do rombo deixado pela quadrilha.



Tela de compra online com Pix. Pessoas podem optar entre código QR ou copiar código dinâmico – Reprodução/Internet

O GoPix circula desde 2023, por meio de campanhas de anúncios fraudulentos no Google Ads.

“Os sites falsos usados na fraude ficam poucas horas no ar e tem um público bem definido”, afirma Fabio Assolini, diretor da equipe de pesquisa da Kaspersky para América Latina.

O gigante das buscas diz que mantém monitoramento ativo de campanhas criminosas. De acordo com o dado mais recente da empresa, o Google tirou do ar, em 2024, 415 milhões de anúncios ligados a fraudes financeiras.

De acordo com Assolini, o vírus ainda tem uma atuação seletiva para desviar grandes valores e deixar menos alertas para o sistema bancário. Antes de executar o golpe, o GoPix pede um “score de rede”, similar a avaliação do Serasa, para testar se aquele computador é de pessoa física ou de uma empresa.

O alvo preferencial dessa quadrilha são as companhias, que

movimentam valores mais altos de uma só vez.

Se o usuário passar nessa triagem, o site oferece o GoPix para download, que simula ser o aplicativo legítimo do serviço que a pessoa buscava (por exemplo, um falso instalador do “WhatsApp Web”).

Caso o usuário não seja considerado um alvo, a opção de baixar o programa malicioso não aparece.

O vírus, uma vez instalado no sistema Windows do computador ou notebook, monitora tudo o que é copiado e colado. Se uma chave Pix, um código de boleto bancário ou um endereço de carteira de criptomoedas for copiado, o GoPix pode alterar esses dados no momento da colagem, redirecionando o dinheiro para os criminosos sem que a vítima perceba.

A alteração dos dados é feita com uma ferramenta chamada Proxy que redireciona o usuário para um servidor local onde estão os comandos para executar o golpe. Assim, os criminosos interceptam e alteram as informações enquanto o usuário navega em sites de bancos legítimos.

Esta recente atualização do Gopix representa um aumento do escopo da quadrilha para incluir pessoas físicas que movimentam altas quantias. As criptomoedas lastreadas no dólar, chamadas de stablecoins, têm popularidade crescente em operações de câmbio e compras de importados online. Em 2025, mais de 90% das transações com criptoativos no Brasil usaram a stablecoin USDT, da empresa Tether.

Segundo Assolini, ainda há menos pistas de como os criminosos operam para desviar boletos. Essa forma de pagamento fica ligada a um CNPJ ou CPF e passa por mais etapas de processamento. Por ora, a Kaspersky encontrou um gatilho para acionar o vírus quando o usuário faz esse tipo de operação.

A quadrilha por trás do GoPix consegue fraudar até o certificado de conexão segura indicado pelo código HTTPS – o

pequeno cadeado ao lado do endereço do site. Para isso, eles usam um certificado digital falso.

COMO SE PROTEGER

- Atente-se ao conteúdo de anúncios patrocinados no Google, especialmente para baixar aplicativos
- Baixe programas apenas nos sites oficiais dos desenvolvedores
- Mantenha antivírus atualizado
- Atualize o Windows e o navegador regularmente
- Antes de confirmar qualquer transferência, verifique se a chave Pix, o código do boleto ou o endereço da carteira não foram alterados

No caso de transações via Pix, é possível contestá-las no app do banco.

Fonte: Folha de São Paulo e Publicado Por: Jornal Folha do Progresso 17/03/2026/07:19:37

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