Notificações do GitHub abusadas para se passar pelo Y Combinator por ro

Data: 2025-09-24 12:43:33

Autor: Inteligência Against Invaders

Uma campanha massiva de phishing direcionada aos usuários do GitHub com drenadores de

criptomoedas, entregues por meio de convites falsos para o programa Y Combinator (YC) W2026.

A Y Combinator é uma aceleradora de startups que financia e orienta projetos em seus estágios iniciais e conecta fundadores a uma rede de ex-alunos e empresas de capital de risco.

O invasor abusou do sistema de notificação do GitHub para entregar as mensagens fraudulentas, criando problemas em vários repositórios e marcando usuários-alvo.

Ao mencionar um nome de conta em um problema, o GitHub envia automaticamente uma notificação. Como o e-mail vem de uma fonte legítima, ele foi direto para a caixa de entrada dos destinatários pretendidos.

A isca usada na campanha foi um convite para se inscrever no Winter 2026 Batch (W2026), a próxima rodada de inscrições para financiamento da YC, supostamente prometendo um total de US$ 15 milhões.

[IMAGEM REMOVIDA]Os desenvolvedores relataram ter visto até 500 problemas abertos a partir de um novo usuário criado há apenas uma semana. No final do problema, o invasor mencionou uma lista de nomes de usuário para receber a notificação.

O BleepingComputer viu uma lista de cerca de 30 usuários-alvo e não parece ser um terreno comum para todos eles, com base nos projetos listados.

No entanto,o objetivo do invasor era roubar criptomoedae é mais provável que um desenvolvedor tenha uma carteira digital.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]

Na realidade, assinar a verificação autoriza transações maliciosas e as carteiras são drenadas dos criptoativos.

[IMAGEM REMOVIDA]está disponível aqui. O prazo para se inscrever nesta rodada é 10 de novembro, e o lote acontecerá no próximo ano em São Francisco entre janeiro e março.

Bill Toulas

Bill Toulas é redator de tecnologia e repórter de notícias de segurança da informação com mais de uma década de experiência trabalhando em várias publicações online, cobrindo código aberto, Linux, malware, incidentes de violação de dados e hacks.

Você também pode gostar: