Hackers roubam dados identificáveis do usuário do Discord em violação d

Data: 2025-10-04 11:16:46

Autor: Inteligência Against Invaders

Os hackers roubaram informações parciais de pagamento e dados de identificação pessoal

associados a alguns usuários do Discord depois de comprometer um provedor de atendimento ao

cliente terceirizado.

O ataque ocorreu em 20 de setembro e afetou “um número limitado de usuários” que interagiram com o suporte ao cliente do Discord e/ou equipes de Confiança e Segurança.

O Discord foi criado como uma plataforma de comunicação para jogadores, que representam mais de 90% da base de usuários, mas se expandiu para várias outras comunidades, permitindo mensagens de texto, bate-papos de voz e videochamadas.

De acordo com as estatísticas da plataforma, mais de 200 milhões de pessoas estão usando o Discord todos os meses.

Hackers exigiram um resgate

Na notificação aos usuários afetados, a empresa de mensagens diz que o ataque ocorreu em 20 de setembro e “uma parte não autorizada obteve acesso limitado a um sistema de atendimento ao cliente de terceiros usado pelo Discord”.

Na sexta-feira, o Discord divulgou o incidente publicamente, dizendo que tomou medidas imediatas para isolar o provedor de suporte de seu sistema de tickets e iniciou uma investigação.

> Isso incluiu revogar o acesso do provedor de suporte ao cliente ao nosso sistema de tíquetes, lançar uma investigação interna, contratar uma empresa líder em computação forense para apoiar nossos esforços de investigação e remediação e envolver a aplicação da lei. Discórdia

O ataque parece ter motivação financeira, já que os hackers exigiram um resgate do Discord em troca de não vazar as informações roubadas.

Os dados expostos incluem informações de identificação pessoal, como nomes reais e nomes de usuário, endereços de e-mail e outros detalhes de contato fornecidos à equipe de suporte.

O serviço de comunicação social diz que endereços IP, mensagens e anexos enviados aos agentes de atendimento ao cliente também foram comprometidos.

Os hackers também acessaram fotos de documentos de identificação emitidos pelo governo (carteira de motorista, passaporte) para um pequeno número de usuários.

Informações parciais de cobrança, como tipo de pagamento, os últimos quatro dígitos do cartão de crédito e histórico de compras associado à conta comprometida, também foram expostas.

[IMAGEM REMOVIDA]observa que o tipo de dados roubados dos usuários do Discord representa “literalmente pessoas [sic] identidade inteira.”

Alon Gal, diretor de tecnologia da empresa de inteligência de ameaças Hudson Rock, acredita que, se os hackers divulgarem os dados do Discord, isso poderá fornecer informações cruciais para ajudar a descobrir ou resolver hacks e golpes de criptomoedas.

“Direi apenas que, se vazar, esse banco de dados será enorme para resolver hacks e golpes relacionados a criptomoedas, porque os golpistas não costumam se lembrar de usar um e-mail e VPN descartáveis e quase todos eles estão no Discord” diz Alon Gal, Diretor de Tecnologia da Hudson Rock

Atualmente, não está claro quantos usuários do Discord são afetados, e o nome do provedor terceirizado ou o vetor de acesso não foi divulgado publicamente.

O BleepingComputer entrou em contato com o Discord com um pedido de mais detalhes sobre o ataque, mas um comentário da plataforma de comunicação social não estava disponível imediatamente.

Vale a pena notar que centenas de empresas tiveram suas instâncias do Salesforce comprometidas depois que o grupo de extorsão ShinyHunters as acessou usando tokens roubados do Salesloft Drift OAuth.

No mês passado, os hackers alegaram ter roubado mais de 1,5 bilhão de registros do Salesforce de 760 empresas.

[IMAGEM REMOVIDA]

Não perca o evento que moldará o futuro da sua estratégia de segurança