Gigante da montadora Stellantis confirma violação de dados após hack do

Data: 2025-09-23 02:43:24

Autor: Inteligência Against Invaders

A gigante automotiva Stellantis confirmou que os invasores roubaram alguns dos dados de seus

clientes norte-americanos depois de obter acesso à plataforma de um provedor de serviços

terceirizado.

A Stellantis é uma corporação multinacional formada em 2021 após a fusão do Grupo PSA (Peugeot Société Anonyme) e da Fiat Chrysler Automobiles (FCA). A Stellantis é atualmente uma das maiores empresas automotivas do mundo em receita e a quinta maior montadora do mundo em volume.

A empresa possui 14 grandes marcas automotivas, incluindo Alfa Romeo, Chrysler, Citroën, Dodge, DS Automobiles, Fiat, Jeep, Lancia, Maserati, Opel, Peugeot, Ram e Vauxhall, e opera fábricas na Europa, América do Norte, América do Sul e outras regiões, com operações em mais de 130 países.

De acordo com um comunicado publicado no fim de semana, os invasores apenas roubaram informações de contato do cliente durante a violação, já que a plataforma comprometida não foi usada para armazenar informações financeiras ou outras informações pessoais confidenciais.

“Recentemente, detectamos acesso não autorizado à plataforma de um provedor de serviços terceirizado que oferece suporte às nossas operações de atendimento ao cliente na América do Norte”, Stellantis ele disse.

“Após a descoberta, ativamos imediatamente nossos protocolos de resposta a incidentes, iniciamos uma investigação abrangente e tomamos medidas imediatas para conter e mitigar a situação. Também estamos notificando as autoridades competentes e informando diretamente os clientes afetados.”

A gigante automobilística também aconselhou os clientes a serem cautelosos com possíveis tentativas de phishing e a evitar clicar em links suspeitos ou compartilhar informações pessoais ao receber e-mails, mensagens de texto ou chamadas inesperadas.

O BleepingComputer entrou em contato com a Stellantis com perguntas sobre o incidente, mas uma resposta não estava disponível imediatamente.

Violação de dados do Salesforce reivindicada porShinyHunters

Embora a Stellantis não tenha compartilhado mais informações sobre esse ataque, o BleepingComputer descobriu que ele faz parte de um recente onda de violações de dados do Salesforce ligado ao grupo de extorsão ShinyHunters, que afetou várias empresas de alto perfil.

Hoje cedo, a ShinyHunters reivindicou a responsabilidade pela violação de dados da Stellantis e disse ao BleepingComputer que havia roubado mais de 18 milhões de registros do Salesforce, incluindo nomes e detalhes de contato, da instância do Salesforce da empresa.

Desde o início do ano, o grupo de extorsão foi visando clientes do Salesforce em ataques de roubo de dados usando ataques de phishing de voz, impactando empresas como Pesquise no Google, Cisco, Qantas, Adidas, Allianz Life, Seguro de Agricultores, Dia de trabalhoe subsidiárias da LVMH, incluindo Dior, Louis Vuittone Tiffany & Co.

ShinyHunters também afirma que usoutokens OAuth roubados para a integração de bate-papo Drift AI da Salesloft com o Salesforce para roubar informações confidenciais, como senhas, chaves de acesso da AWS e tokens Snowflake, após obter acesso às instâncias do Salesforce dos clientes.

Usando esse método, eles alegaram ter roubado informações de clientes dePesquise no Google, Cloudflare, Zscaler, Sustentável, Redes de Palo Alto,CyberArk, Nutanix, Qualys, Rubrik, Elástico, Além da confiança, Ponto de prova, JFrog,Redes Catoe muitos mais.

Na semana passada, o FBI divulgou um alerta Flash compartilhamento de IOCs descobertos durante os ataques e alerta sobre agentes de ameaças que violam os ambientes Salesforce das organizações para roubar dados e extorquir vítimas. Enquanto isso, o grupo de extorsão disse ao BleepingComputer que eles roubaram mais de 1,5 bilhão de registros do Salesforce de 760 empresas, usando tokens Salesloft Drift OAuth comprometidos.

[IMAGEM REMOVIDA]