ShinyHunters lança site de vazamento de dados do Salesforce para extorq

Data: 2025-10-03 18:30:31

Autor: Inteligência Against Invaders

Um grupo de extorsão lançou um novo site de vazamento de dados para extorquir publicamente dezenas de empresas afetadas por um onda de violações do Salesforce, vazando amostras de dados roubados nos ataques.

Os agentes de ameaças responsáveis por esses ataques afirmam fazer parte dos grupos ShinyHunters, Scatter Spider e Lapsus$, referindo-se coletivamente a si mesmos como “Scattered Lapsus$ Hunters”.

Hoje, eles lançaram um novo site de vazamento de dados contendo 39 empresas afetadas pelos ataques. Cada entrada inclui amostras de dados supostamente roubados das instâncias do Salesforce das vítimas e avisa as vítimas para entrar em contato para “impedir a divulgação pública” de seus dados antes que o prazo de 10 de outubro seja atingido.

As empresas que estão sendo extorquidas no site de vazamento de dados incluem marcas e organizações conhecidas, incluindo FedEx, Disney/Hulu, Home Depot, Marriott, Google, Cisco, Toyota, Gap, McDonald’s, Walgreens, Instacart, Cartier, Adidas, Sake Fifth Avenue, Air France & KLM, Transunion, HBO MAX, UPS, Chanel e IKEA.

“Todos eles foram contatados há muito tempo, eles viram o e-mail porque eu os vi baixar as amostras várias vezes. A maioria deles optou por não divulgar e ignorar”, disse ShinyHunters ao BleepingComputer.

“É altamente recomendável que você tome a decisão certa, sua organização pode impedir a divulgação desses dados, recuperar o controle sobre a situação e todas as operações permanecem estáveis como sempre. É altamente recomendável que um tomador de decisão se envolva, pois estamos apresentando uma oportunidade clara e mutuamente benéfica para resolver esse assunto”, alertaram no site do vazamento.

Os agentes de ameaças também adicionaram uma entrada separada solicitando que a Salesforce pague um resgate para evitar que todos os dados dos clientes afetados (aproximadamente 1 bilhão de registros contendo informações pessoais) vazem.

“Se você cumprir, nos retiraremos de qualquer negociação ativa ou pendente individualmente de seus clientes. Seus clientes não serão atacados novamente nem enfrentarão um resgate nosso novamente, caso você pague”, acrescentaram.

O grupo de extorsão também ameaçou a empresa, afirmando que ajudaria os escritórios de advocacia a entrar com ações civis e comerciais contra a Salesforce após as violações de dados e alertou que a empresa também falhou em proteger os dados dos clientes, conforme exigido pelo

Regulamento Geral de Proteção de Dados Europeu (GDPR).

[IMAGEM REMOVIDA]visando clientes do Salesforce com ataques de phishing de voz desde o início do ano, levando a violações que impactaram empresas como Pesquise no Google, Cisco, Qantas, Adidas, Allianz Life, Seguro de Agricultores, Dia de trabalho, bem como subsidiárias da LVMH, incluindo Dior, Louis Vuittone Tiffany & Co.

Nesses ataques, os agentes de ameaças enganaram os funcionários para vincular um aplicativo OAuth malicioso à instância do Salesforce de sua empresa. A ShinyHunters disse ao BleepingComputer que, embora uma instância específica do Salesforce possa ter sido direcionada, ela também continha dados de muitas das subsidiárias, tornando os ataques mais impactantes.

Uma vez conectados, os invasores roubaram bancos de dados da empresa e usaram os dados para extorquir as vítimas por e-mail. Esses e-mails de extorsão foram assinados por ShinyHunters, um notório grupo de extorsão ligado a uma longa série de violações de alto perfil nos últimos anos, incluindo o Ataques de floco de neve e aqueles contra AT&T e Escola de Energia.

Caçadores brilhantestambém alegou ter usado tokens OAuth roubados para a integração de bate-papo Drift AI da Salesloft com o Salesforce para roubar informações confidenciais, incluindo senhas, chaves de acesso da AWS e tokens Snowflake, das instâncias do Salesforce dos clientes.

Esses ataques foram rastreados pela Mandiant em um cluster de ameaças separado chamado “UNC6395”, pois eles não conseguiram vincular formalmente as violações a esse grupo.

Em um canal do Telegram associado ao grupo de extorsão, os agentes de ameaças afirmam que começarão a extorquir empresas afetadas pelos ataques do Salesloft Drift em um site separado de vazamento de dados lançado em 10 de outubro.

A ShinyHunters disse anteriormente ao BleepingComputer que os ataques de roubo de dados da Salesloft afetaram aproximadamente 760 empresas e resultaram emo roubo de 1,5 bilhão de registros do Salesforce.

Os ataques do Salesloft são conhecidos por terem impactadoPesquise no Google, Redes de Palo Alto, CyberArk, Cloudflare, Rubrik, Elástico, Além da confiança, Ponto de prova, JFrog, Zscaler, Sustentável, Nutanix, QualyseRedes Cato,entre muitos outros. Os ShinyHunters afirmam que as empresas não serão extorquidas novamente sob a campanha Salesloft se um resgate for pago nesta fase inicial de extorsão.

“Estamos cientes das recentes tentativas de extorsão por agentes de ameaças, que investigamos em parceria com especialistas e autoridades externas. Nossas descobertas indicam que essas tentativas estão relacionadas a incidentes passados ou infundados, e continuamos engajados com os clientes afetados para fornecer suporte”, Salesforce disse em um comunicado publicado depois que ShinyHunters lançou seusite de vazamento de dados.

“Neste momento, não há indicação de que a plataforma Salesforce tenha sido comprometida, nem essa atividade está relacionada a qualquer vulnerabilidade conhecida em nossa tecnologia.”

Atualização03 de outubro, 11:02 EDT: Adicionada declaração do Salesforce.

[IMAGEM REMOVIDA]

O Evento de Validação de Segurança do Ano: O Picus BAS Summit

Junte-se ao **Cúpula de Simulação de Violação e Ataque** e experimente o **Futuro da validação de segurança**. Ouça os principais especialistas e veja como **BAS alimentado por IA** está transformando a simulação de violação e ataque.

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