A Gangue Qilin Ransomware Reivindica o Ataque Cibernético da Asahi

Data: 2025-10-07 18:15:00

Autor: Inteligência Against Invaders

O grupo de ransomware Qilin reivindicou a responsabilidade pelo ataque cibernético ao Asahi Group

do Japão e diz que roubou dados confidenciais da empresa.

Site do consumidor Revelada a Comparitech que o notório ator listou a Asahi em seu site de vazamento de dados em 7 de outubro, alegando ter roubado 27 GB de arquivos da empresa.

Os dados supostamente incluem detalhes pessoais de funcionários, bem como informações comerciais confidenciais da Asahi. Isso inclui documentos financeiros, orçamentos, contratos, planos e previsões de desenvolvimento.

A Asahi não respondeu às alegações de Qilin no momento da redação deste artigo.

A atualização vem poucos dias depois que a Asahi confirmou que havia caído vítima de um ataque de ransomware, o que resultou em uma “transferência não autorizada de dados” de seus servidores.

O ataque causou interrupções operacionais significativas na cervejaria, com Pedido e envio as operações no Japão foram imediatamente suspensas enquanto a empresa montava sua resposta. Além disso, as operações do call center, incluindo balcões de atendimento ao cliente, foram suspensas.

A Asahi está em processo de retomada das operações, incluindo o lançamento de pedidos manuais e processos de envio.

A empresa com sede em Tóquio possui uma variedade de marcas globais de bebidas conhecidas, alcoólicas e não alcoólicas, além de produtos alimentícios.

Suas cinco marcas de cerveja são Asahi, Peroni, Kozer, Pilsner Urquell e Grolsch. Também é proprietária da cervejaria Fullers, com sede no Reino Unido.

Qilin Liderando o Caminho em Ransomware

A gangue Qilin emergiu como o ator de ransomware mais prolífico em um mercado cada vez mais lotado nos últimos meses.

ZeroFox *Resumo do ransomware no 3º trimestre de 2025* descobriu que Qilin reivindicou a responsabilidade pelo maior número de ataques no trimestre, com 227.

Grupo NCC reportado que o Qilin representou 16% de todos os ataques de ransomware em agosto de 2025, tornando-se o grupo de ameaças mais ativo no mês.

De acordo com a Comparitech, a Qilin assumiu o crédito por três outros ataques de ransomware confirmados em empresas japonesas este ano: Shinko Plastics em junho, Nissan Creative Box em agosto e Osaki Medical em agosto.

Leia agora: Qilin reivindica ataque de ransomware às escolas de Mecklenburg

O operador de ransomware como serviço (RaaS) fornece ferramentas e infraestrutura de ransomware para afiliados, recebendo uma participação de 15 a 20% nos pagamentos de resgate.

Ele instrui explicitamente seus afiliados a não visar sistemas localizados em países que fazem parte da Comunidade de Estados Independentes (CEI), incluindo Rússia e Bielorrússia.

Ele supostamente opera uma infraestrutura tecnicamente madura, com malware personalizado escrito em Rust e C para ataques multiplataforma, incluindo sistemas Windows, Linux e ESXi.

Crédito da imagem: Shaun no Japão / Shutterstock.com