ShinyHunters viola Gucci, Balenciaga e Alexander McQueen: US$ 7,4 milh

Data: 2025-09-17 10:20:01

Autor: Inteligência Against Invaders

Redazione RHC**:17 setembro 2025 10:31**

A Kering, gigante do luxo e da moda, anunciou oficialmente que uma violação de dados foi perpetrada contra clientes de suas marcas líderes, incluindo **Gucci, Balenciaga e Alexander McQueen.** ShinyHunters, os mesmos agentes de ameaças que entrevistamos recentemente, conseguiram acessar as informações privadas dos usuários.

A violação, detectada em junho, mas ocorrida em abril, expôs informações de identificação pessoal (PII) de aproximadamente 7,4 milhões de endereços de e-mail exclusivos.

Nenhum dado regulado pelo padrão PCI-DSS, como números de cartão de crédito ou detalhes de contas bancárias, foi exfiltrado. Em vez disso, os arquivos incluem nomes, endereços de e-mail, números de telefone, endereços de entrega e um campo “Total de vendas” indicando os gastos acumulados de cada cliente.

A BBC relata que o agressor, que se identificou como Shiny Hunters, alegou ter **negociou um resgate em Bitcoin (BTC) com a Kering a partir de junho via Telegram.** A Kering nega qualquer negociação de resgate e confirma que está aderindo às diretrizes de aplicação da lei que exigem a recusa de pagamentos de resgate.

De acordo com a declaração da Kering, o invasor obteve acesso temporário não autorizado por meio de credenciais internas comprometidas, provavelmente coletadas por meio de uma campanha de phishing direcionada aos portais SSO da Salesforce. O conjunto de dados roubado contém:

- E-mail
- Nome e sobrenome
- Número telefônico
- Endereço de entrega
- Vendas totais

A análise de uma amostra de prova de conceito revelou que os gastos variam de **$ 10.000 a $ 86.000 por pessoa,** preocupações crescentes sobre spear-phishing. A Kering notificou as autoridades de proteção de dados relevantes de acordo com o Artigo 33 do GDPR e se comunicou diretamente com os clientes afetados por e-mail.

Da mesma forma, o Grupo de Análise de Ameaças do Google atribui uma campanha semelhante, identificada como UNC6040, ao Shiny Hunters, observando a exploração de tokens de API roubados e o uso indevido de escopos OAuth para coletar credenciais de outras grandes empresas.

Todos os clientes são aconselhados a redefinir suas senhas e revisar suas configurações de recuperação de conta para todos os perfis de e-mail e comércio eletrônico. Estar alerta para chamadas ou e-mails não solicitados solicitando ação urgente pode ajudar a evitar fraudes subsequentes.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli