# E-mails de extorsão enviados a executivos por autoproclamado membro d

Data: 2025-10-02 15:45:00

Autor: Inteligência Against Invaders

Um indivíduo ou grupo de pessoas que afirmam estar trabalhando com o ransomware Clop tem

enviado e-mails de extorsão para executivos de várias organizações desde 29 de setembro, de

acordo com o Google.

O agente da ameaça também afirma ter roubado dados confidenciais de seu alvo Oracle E-Business Suite.

Pesquisadores da Mandiant e do Google Threat Intelligence Group (GTIG) estão investigando um caso, mas ainda não reuniram evidências suficientes para fundamentar as alegações do indivíduo.

Charles Carmakal, CTO da Mandiant no Google Cloud, comentou: “No momento, estamos observando uma campanha de e-mail de alto volume sendo lançada a partir de centenas de contas comprometidas”.

A análise inicial de sua equipe confirma que pelo menos uma dessas contas foi anteriormente associada à atividade do FIN11, um grupo de ameaças com motivação financeira de longa data, conhecido por implantar ransomware e se envolver em extorsão.

“Os e-mails maliciosos contêm informações de contato e verificamos que os dois endereços de contato específicos fornecidos também estão listados publicamente no site de vazamento de dados do Clop (DLS). Esse movimento sugere fortemente que há alguma associação com a Clop e eles estão aproveitando o reconhecimento da marca para sua operação atual”, acrescentou Carmakal.

No entanto, ele observou que isso não significa necessariamente que Clop esteja envolvido ou mesmo ciente da campanha.

“A atribuição no espaço do crime cibernético com motivação financeira é muitas vezes complexa, e os atores frequentemente imitam grupos estabelecidos como o Clop para aumentar a alavancagem e a pressão sobre as vítimas. Recomendamos que as organizações-alvo investiguem seus ambientes em busca de evidências de atividade de agentes de ameaças”, concluiu.