Google alerta para campanha de extorsão Cl0p contra usuários do Oracle

Data: 2025-10-03 06:02:56

Autor: Inteligência Against Invaders

Google alerta para campanha de extorsão Cl0p contra usuários do Oracle E-Business

O Google observou o grupo de ransomware Cl0p enviando e-mails de extorsão para executivos, alegando roubo de dados do Oracle E-Business Suite.

Pesquisadores do Google Mandiant e do Google Threat Intelligence Group (GTIG) estão rastreando um suspeito Cl0p ransomware atividade do grupo, onde os agentes de ameaças tentam extorquir executivos com alegações de roubo de dados do Oracle E-Business Suite.

“Um grupo de hackers alegou ter violado o E-Business Suite da Oracle, que executa operações principais, incluindo finanças, cadeia de suprimentos e gerenciamento de relacionamento com o cliente. Em um caso, eles exigiram um resgate de até US$ 50 milhões, de acordo com a empresa de segurança cibernética Halcyon, que atualmente está respondendo à campanha. O grupo, que afirma ser afiliado a uma organização criminosa chamada Cl0p, forneceu provas de comprometimento às vítimas, incluindo capturas de tela e árvores de arquivos. relatou Bloomberg*.*

“Pelo menos uma empresa confirmou que os dados de seus sistemas Oracle foram roubados, de acordo com uma das pessoas.”

Os invasores provavelmente invadiram e-mails de usuários e exploraram a redefinição de senha padrão do Oracle E-Business Suite para roubar credenciais válidas, informou a empresa de segurança cibernética Halycon.

“Vimos o Cl0p exigir enormes resgates de sete e oito dígitos nos últimos dias”, disse Cynthia Kaiser, vice-presidente do centro de pesquisa de ransomware da Halcyon. “Este grupo é notório pelo roubo furtivo de dados em massa que aumenta sua influência nas negociações de resgate.”

“Esta atividade começou em ou antes de 29 de setembro de 2025, mas os especialistas da Mandiant ainda estão nos estágios iniciais de várias investigações e ainda não comprovaram as alegações feitas por este grupo”, dito *Genevieve Stark, Chefe de Análise de Inteligência de Operações de Informação e Crimes Cibernéticos da GTIG.*

Stark disse que um e-mail nas notas de extorsão está vinculado a uma afiliada da Cl0p e inclui contatos do site Cl0p, mas o Google não tem provas para confirmar as alegações dos invasores.

O CTO da Mandiant, Charles Carmakal, disse que os invasores usam centenas de contas hackeadas em uma campanha de extorsão em massa. Pelo menos uma conta está vinculada ao

grupo de hackers com motivação financeira FIN11.

“Atualmente, estamos observando uma campanha de e-mail de alto volume sendo lançada a partir de centenas de contas comprometidas e nossa análise inicial confirma que pelo menos uma dessas contas foi anteriormente associada à atividade do FIN11, um grupo de ameaças financeiramente motivado de longa data conhecido por implantar ransomware e se envolver em extorsão”, disse Carmakal.

Desde agosto de 2020, o FIN11 tem como alvo organizações em muitos setores, incluindo defesa, energia, finanças, saúde, jurídico, farmacêutico, telecomunicações, tecnologia e transporte. O grupo de extorsão foi observado implantando oClop ransomwarenas redes de suas vítimas.

Os pesquisadores acreditam que o FIN11 opera a partir da Comunidade de Estados Independentes (CEI – países da antiga União Soviética). Em 2020, os especialistas da Mandiant observaram metadados de arquivos em russo no código do malware e relataram que o ransomware Clop foi implantado apenas em máquinas com layout de teclado usado fora dos países da CEI.

Na época, pesquisadores da Mandiant da FireEye observaram hackers do FIN11 usando mensagens de spear-phishing para distribuir um downloader de malware apelidado de FRIENDSPEAK.

“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 Cl0p (DLS)”, acrescentou Carmakal. “Esse movimento sugere fortemente que há alguma associação com a Cl0p, e eles estão aproveitando o reconhecimento da marca para sua operação atual.”

Halcyon, citando pessoas familiarizadas com o assunto, revelou acreditar que os agentes de ameaças exploraram uma vulnerabilidade no E-Business Suite da Oracle.

Os pesquisadores da Mandiant recomendam investigar seu ambiente em busca de indicadores de comprometimento associados à operação Cl0p.

Cl0p lançou grandes ataques nos últimos anos, explorando falhas de dia zero em softwares populares, como Aceleração, SolarWinds, Fortra GoAnywheree MOVER.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPagAnini

(Assuntos de Segurança–hacking,ransomware)