Lunaloock Ransomware atacando artistas a roubar e criptografar dados - A

Data: 2025-09-08 16:31:01

Autor: Inteligência Against Invaders

A Lunaloock, uma tensão de ransomware recém -surgida, lançou uma campanha direcionada contra artistas independentes e seus clientes, exigindo um resgate pesado em troca de obras criativas roubadas e dados pessoais vazados.

Emergindo no início de setembro de 2025, o Lunaloock Group reivindica a responsabilidade de violar artistas e clientes, um mercado digital popular onde os ilustradores se conectam com os clientes que buscam obras de arte personalizadas.

[Relatórios](#) Indique que os operadores da Lunaloock exploraram uma vulnerabilidade crítica no serviço de desktop remoto de artistas e clientes, causando tempo limite generalizado de conexão e erros de hospedagem no final de 6 de setembro de 2025.

Os usuários que tentam acessar a plataforma foram recebidos com uma mensagem de “conexão cronometrada” da CloudFlare, revelando um “erro do host” que renderizou o navegador e as infraestruturas de nuvem operacionais – confirmando a violação no próprio aplicativo. Logo depois, um aviso de resgate apareceu na página de login do site, aviso:

O relógio da contagem regressiva exibiu ameaçadoramente 4 dias, 8 horas, 11 minutos e 6 segundos, ressaltando a urgência da ameaça.

O grupo ameaçou ainda que, se o resgate permanecesse não remunerado, todas as obras de arte seriam enviadas aos conjuntos de dados de treinamento de IA vendidos para as principais empresas de tecnologia – uma tática alarmante que armazinha o conteúdo criativo contra seus criadores.

Impacto em artistas independentes

O foco de Lunaloock em uma comunidade de nicho diferencia esta campanha dos ataques de ransomware de broto.

Ao se infiltrar em uma plataforma dedicada a comissões de arte, os invasores de propriedade de propriedade intelectual de alto valor: ilustrações inacabadas, resumos de clientes, detalhes do contrato e informações bancárias para processamento de pagamentos.

O vazamento de tais dados não apenas compromete os meios de subsistência dos artistas, mas também expõe a privacidade pessoal e financeira dos clientes.

Vários ilustradores relataram perder o acesso a seus portfólios, arquivos da comissão e históricos de bate -papo com clientes.

Um artista de conceito freelancer descreveu o ataque como uma “violação da confiança”, observando que meses de esboços e referências confidenciais agora eram mantidos como reféns.

Outro criador lamentou: “Não se trata apenas do dinheiro – eles ameaçam entregar nosso trabalho às empresas de IA, desvalorizando nossa criatividade”.

Pesquisadores de segurança da Venarix, uma startup de inteligência de ameaças cibernéticas que oferecem serviços de monitoramento gratuitos para comunidades vulneráveis, começaram a analisar os padrões de código e mensagens de Lunalock.

As notas de resgate refletem as de alto perfil [Ransomware](#) As famílias, mas incorporam marcas únicas em torno de imagens lunares, sugerindo um esforço deliberado para estabelecer uma franquia de extorsão reconhecível.

Os analistas da Venarix recomendam que as organizações afetadas não se envolvam diretamente com os atacantes nem tentam negociar por meio de canais não verificados.

Em vez disso, eles pedem contenção imediata: isolem servidores infectados, preservam logs para análise forense e consultam empresas de resposta a incidentes especializadas em setores criativos e de mídia.

Mitigações

Os operadores de Lunalock aproveitam popular [criptomoeda](#) Misturadores para ofuscar transações, complicando a capacidade da aplicação da lei de rastrear pagamentos.

Após a violação, artistas e clientes fecharam temporariamente seu serviço para implementar patches de emergência e conduzir uma auditoria de segurança completa.

A liderança da plataforma emitiu um pedido de desculpas público e prometeu reembolsar os custos de hospedagem de comissão, enquanto oferecem extensões gratuitas de assinatura para recuperar a confiança do usuário.

Os voluntários independentes da CyberSec mobilizaram -se nas mídias sociais, usando a hashtag #lunock para compartilhar dicas de mitigação:

- **Práticas de backup:** Armazene arquivos críticos em sistemas de backup offline ou imutáveis ??para impedir que a criptografia de ransomware.
- **Segmentação de rede:** Limite o movimento lateral isolando bancos de dados de produção e repositórios de código por trás dos firewalls endurecidos.
- **Autenticação multifatorial:** Aplicar o MFA em todos os logins administrativos e no nível da conta para reduzir o risco de roubo de credenciais.

Artistas e clientes são incentivados a revisar qualquer atividade incomum da conta e alterar senhas imediatamente. Aqueles que procuram alertas de ameaças proativos podem se inscrever gratuitamente na plataforma de Venarix.

À medida que as gangues de ransomware visam cada vez mais as indústrias criativas, o incidente de Lunalock destaca uma mudança preocupante: os atacantes veem os criadores independentes como presas lucrativas.

A vigilância, a higiene de segurança robusta e a colaboração da comunidade continuam sendo as melhores defesas contra essa ameaça emergente.

A resposta rápida dos artistas e clientes pode ajudar a conter os danos, mas o ecossistema mais amplo deve se preparar para incursões futuras, pois grupos de ransomware refinam suas táticas contra setores especializados.

Encontre esta história interessante! Siga -nos [LinkedIn](#) [X](#) Para obter mais atualizações instantâneas.