Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

LUNALOCK EL NUEVO RANSOMWARE QUE ROBA Y ENCRIPTA EL TRABAJO DE LOS ARTISTAS

08/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

Un nuevo informe de ciberseguridad ha revelado una campaña de ransomware particularmente agresiva. El grupo LunaLock ha atacado la plataforma de encargo de arte Artists & Clients, que conecta a artistas independientes con clientes.

LUNALOCK EL NUEVO RANSOMWARE QUE ROBA Y ENCRIPTA EL TRABAJO DE LOS ARTISTAS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/09/2025
Es día cero (0 day):	No

RESUMEN

Un nuevo informe de ciberseguridad ha revelado una campaña de ransomware particularmente agresiva. El grupo LunaLock ha atacado la plataforma de encargo de arte Artists & Clients, que conecta a artistas independientes con clientes. El ataque ocurrió el 30 de agosto de 2025. Una nota apareció en la web de la empresa, indicando que todo el contenido, incluyendo obras de arte, bases de datos, código fuente y datos personales, fue robado y cifrado. LunaLock exige un rescate de 50.000 dólares en Bitcoin o Monero.

Lo más impactante de este ataque es la amenaza adicional. Los atacantes declararon que, de no recibir el pago, enviarían todas las obras robadas a empresas de IA para que las usaran como conjuntos de datos de entrenamiento. Esta es una forma de extorsión inédita en el mundo del ransomware y representa una amenaza directa a la propiedad intelectual.

Mecanismos de infección y propagación

El ataque de LunaLock utiliza tácticas avanzadas y bien pensadas para infiltrarse y expandirse dentro de la red.

- Spear-phishing dirigido: Los atacantes se hicieron pasar por notificaciones de regalías para engañar a los artistas y lograr que descargaran facturas “infectadas”.
- Recolección de datos: Una vez dentro del sistema, el malware inicia un escaneo exhaustivo para recopilar activos artísticos y datos de los clientes mientras prepara el cifrado.
- Movimiento lateral: Roban tokens de aplicaciones como Microsoft Teams y Slack, lo que les facilita moverse dentro de repositorios compartidos o herramientas de gestión de proyectos.
- Doble extorsión: Los archivos afectados (como .psd o .ai) son cifrados con la extensión. lunalock y luego exfiltrados a un servidor de Comando y Control (C2) antes de solicitar el rescate, duplicando la presión sobre las víctimas.

Ingenio técnico y evasión

LunaLock no solo es un ransomware destructivo; También es un malware diseñado para evadir las defensas.

- Utiliza un cargador personalizado que resuelve dinámicamente las llamadas a la API mediante XOR, lo que complica el análisis estático.
- Implemente la persistencia a través de una tarea oculta llamada “SysUpdate”, lo que asegura que se ejecutará en cada reinicio del sistema.
- Incluye un módulo de JavaScript minificado que desactiva el escaneo en tiempo real de Windows Defender al inyectarse en el Service Control Manager.

Riesgos específicos para artistas digitales

Además del cifrado clásico, el robo y posible uso de sus obras en modelos de IA representa una amenaza directa a la propiedad intelectual y la integridad creativa de los artistas. A ellos no solo les preocupa recuperar sus archivos, sino también evitar que su estilo o portafolio sea explotado por plataformas de IA sin su consentimiento.

RECOMENDACIONES

- Restrinja el intercambio de archivos y tokens entre plataformas como Teams, Slack y los repositorios de tu empresa.
- Vigila las exfiltraciones a través de HTTP y el acceso anómalo a tokens o repositorios.
- Utilice herramientas de seguridad que identifiquen procesos inusuales, cifrado masivo o un modus operandi similar.

NOTICIA COMPLETA

https://devel.group/blog/lunalock-el-nuevo-ransomware-que-roba-y-encripta-el-trabajo-de-los-artistas/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group