Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMWARE IMPULSADO POR IA: PROMPTLOCK MARCA UNA NUEVA ERA DE CIBERATAQUES

27/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Un grupo de investigadores de ciberseguridad ha identificado lo que podría considerarse el primer ransomware impulsado por inteligencia artificial (IA), denominado PromptLock. Aunque aún no se ha visto en ataques reales, esta prueba de concepto es muy preocupante porque marca una nueva era en las ciberamenazas. Utilizar IA para generar malware en tiempo real rompe con los modelos de ataque tradicionales.

RANSOMWARE IMPULSADO POR IA: PROMPTLOCK MARCA UNA NUEVA ERA DE CIBERATAQUES

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

ID de alerta:	DSOC-CERT_2025_08_27_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	27/08/2025
Es día cero (0 day):	No

RESUMEN

Un grupo de investigadores de ciberseguridad ha identificado lo que podría considerarse el primer ransomware impulsado por inteligencia artificial (IA), denominado PromptLock. Aunque aún no se ha visto en ataques reales, esta prueba de concepto es muy preocupante porque marca una nueva era en las ciberamenazas. Utilizar IA para generar malware en tiempo real rompe con los modelos de ataque tradicionales.

¿Cómo funciona PromptLock?

- Modelo de IA local: El ransomware ejecuta un modelo de lenguaje (GPT-OSS:20B) de OpenAI de forma local a través de la API Ollama. Esto significa que no depende de conexiones a la nube, lo que lo hace más difícil de rastrear.
- Generación dinámica de scripts: La IA crea scripts maliciosos de Lua “al vuelo”, adaptándolos a cada entorno de manera específica.
- Funciones maliciosas automatizadas: Estos scripts pueden inspeccionar el sistema de archivos, exfiltrar datos, encriptar contenidos usando el algoritmo SPECK de 128 bits e, incluso, se anticipa que podría incluir funciones más destructivas en el futuro.
- Compatibilidad multiplataforma: Está programado en Golang, lo que lo hace compatible con sistemas operativos como Windows, macOS y Linux, dándole un alcance muy amplio.
- Detección reducida: Como el malware es generado dinámicamente, los indicadores de compromiso (IoC) cambian con cada ejecución. Esto dificulta su detección por métodos tradicionales, como las firmas de antivirus.

¿Por qué es una amenaza tan importante?

PromptLock demuestra que la IA se está usando para generar malware modular y adaptable sobre la marcha, y no solo para crear phishing o deepfakes. Al automatizar tareas como la exploración, exfiltración y encriptación, esta herramienta reduce la barrera técnica para los atacantes.

Aunque es solo un prototipo, este desarrollo podría escalar rápidamente hacia amenazas mucho más sofisticadas y comunes. La aparición de PromptLock es una alerta temprana para que las organizaciones y los gobiernos impulsen la adopción de soluciones de ciberseguridad basadas en IA, así como marcos regulatorios y éticos para limitar el uso de estas tecnologías con fines criminales.

RECOMENDACIONES

- Mantén tus sistemas siempre actualizados: Asegúrate de que los sistemas operativos, aplicaciones y soluciones de seguridad estén siempre con los últimos parches.
- Automatiza las actualizaciones: Configura el despliegue automático de actualizaciones críticas en servidores y endpoints.
- Realiza backups frecuentes: Haz copias de seguridad de tus datos y guárdalas fuera de línea o en entornos aislados (air-gapped).
- Prueba la restauración: Verifica periódicamente que tus backups se puedan restaurar de manera efectiva en un escenario de ataque real.

NOTICIA COMPLETA

https://devel.group/blog/ransomware-impulsado-por-ia-promptlock-marca-una-nueva-era-de-ciberataques/

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