Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVA AMENAZA EN GMAIL CON IA DE GOOGLE

29/ 08 / 2025

CONTENIDO

INTRODUCCIÓN 3

RESUMEN 5

NOTICIA COMPLETA 6

CONTACTOS DE SOPORTE 6

INTRODUCCIÓN

La adopción de herramientas de inteligencia artificial en plataformas de uso cotidiano, como Gmail, ha transformado la manera en que los usuarios gestionan su información. Sin embargo, esta misma tecnología está abriendo nuevas oportunidades para los ciberdelincuentes, que ahora encuentran en los asistentes de IA un medio para ejecutar ataques más sofisticados y difíciles de detectar.

Recientemente, Google emitió una alerta crítica tras descubrir un ataque que explota a su asistente Gemini dentro de Gmail mediante una técnica de inyección indirecta de instrucciones. Esta amenaza representa un punto de inflexión en la ciberseguridad, ya que demuestra cómo los atacantes pueden manipular las funciones automatizadas de la IA para engañar a los usuarios sin necesidad de enlaces maliciosos o archivos adjuntos tradicionales.

NUEVA AMENAZA EN GMAIL CON IA DE GOOGLE

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

ID de alerta:	DSOC-CERT_2025_08_29_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	29/08/2025
Es día cero (0 day):	No

RESUMEN

Google ha emitido una advertencia tras descubrirse un nuevo tipo de ataque que aprovecha su asistente de inteligencia artificial, Gemini, integrado en Gmail. Este hallazgo confirma cómo la inteligencia artificial está dejando de ser únicamente una herramienta defensiva para convertirse también en un vector de ataque.

¿Cómo funciona la amenaza?
El ataque se basa en una técnica conocida como inyección indirecta de instrucciones:

- Los atacantes insertan texto oculto dentro de los correos electrónicos (por ejemplo, texto blanco sobre fondo blanco).
- Cuando el asistente Gemini resume el correo, interpreta esas instrucciones ocultas.
- Como resultado, el usuario recibe mensajes manipulados que pueden incluir falsas alertas de seguridad o solicitudes de cambio de contraseña.

Lo más preocupante es que no es necesario hacer clic en un enlace ni abrir un archivo adjunto; el riesgo aparece únicamente al utilizar la función de resumen automático.

Implicaciones para la ciberseguridad
Este tipo de ataques marca un punto de inflexión en la gestión del riesgo:

- La inteligencia artificial se incorpora ahora a la superficie de ataque.
- Los controles tradicionales de phishing, como filtros de enlaces o archivos adjuntos, no resultan efectivos frente a estas manipulaciones.
- La confianza en los resultados generados por la IA puede convertirse en una vulnerabilidad crítica.
- La capacidad de automatización de los atacantes permite escalar este tipo de incidentes a gran velocidad.

Recomendaciones para los usuarios

- No confiar ciegamente en resúmenes automáticos que soliciten cambios de credenciales o acciones sensibles.
- Validar siempre la información directamente en las configuraciones de la cuenta, evitando depender exclusivamente de lo que sugiera un asistente de IA.
- Mantenerse informado sobre las nuevas técnicas de ataque que involucran inteligencia artificial.

Conclusión
El surgimiento de ataques basados en inteligencia artificial en entornos tan comunes como Gmail plantea nuevos desafíos de seguridad. La protección ya no se limita a identificar correos sospechosos, sino también a analizar y cuestionar las recomendaciones generadas por herramientas de IA.
La prevención y la educación del usuario serán claves para mitigar estos riesgos, reforzando la resiliencia de organizaciones y usuarios frente a un panorama de amenazas en constante evolución.

NOTICIA COMPLETA

https://devel.group/blog/nueva-amenaza-en-gmail-con-ia-de-google/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

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/