BOLETÍN INFORMATIVO N°207

NOVIEMBRE 2025

Se ha descubierto el malware GlassWorm en tres extensiones de VS Code con miles de instalaciones.

Investigadores de ciberseguridad han revelado un nuevo conjunto de tres extensiones asociadas con la campaña GlassWorm, lo que indica continuos intentos por parte de los actores de amenazas de atacar el ecosistema de Visual Studio Code (VS Code).

Ataques de phishing a gran escala de ClickFix tienen como objetivo los sistemas hoteleros con el malware PureRAT.

Investigadores de ciberseguridad han alertado sobre una campaña masiva de phishing dirigida al sector hotelero que atrae a gerentes de hoteles a páginas al estilo ClickFix y roba sus credenciales mediante el despliegue de malware como PureRAT .

Una grave vulnerabilidad en la CLI de React Native expuso a millones de desarrolladores a ataques remotos.

Han surgido detalles sobre una falla de seguridad crítica, ahora corregida, en el popular paquete npm ” @react-native-community/cli ” que podría ser explotada potencialmente para ejecutar comandos maliciosos del sistema operativo (SO) bajo ciertas condiciones.

Fallos en Microsoft Teams permiten a los atacantes suplantar la identidad de compañeros y editar mensajes sin ser detectados.

Investigadores de ciberseguridad han revelado detalles de cuatro fallos de seguridad en Microsoft Teams que podrían haber expuesto a los usuarios a graves ataques de suplantación de identidad e ingeniería social.

Múltiples vulnerabilidades de Django permiten la inyección SQL y ataques DoS

Django, uno de los frameworks de desarrollo web de Python más populares, ha revelado dos vulnerabilidades de seguridad críticas que podrían permitir a los atacantes ejecutar ataques de inyección SQL y lanzar ataques de denegación de servicio.

RECOMENDACIONES

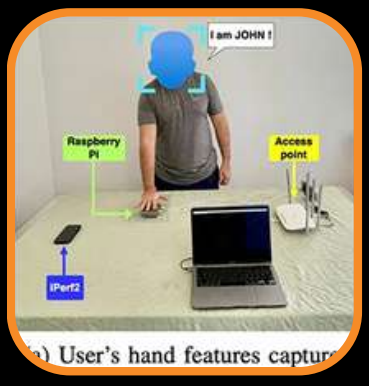
LECTURA DE SEGURIDAD

Cómo adoptar herramientas de seguridad de IA sin perder el control

En este vídeo de Help Net Security, Josh Harguess, CTO de Fire Mountain Labs , explica cómo evaluar, implementar y gestionar herramientas de seguridad basadas en IA. Habla sobre el papel cada vez más importante de la IA en las operaciones de seguridad y los nuevos tipos de riesgos que conlleva.

Resumen semanal: Malware de Hyper-V, bots maliciosos de IA, vulnerabilidades de RDP, bloqueo de WhatsApp y más

Las ciberamenazas no disminuyeron la semana pasada, y los atacantes son cada vez más sofisticados. Estamos viendo malware oculto en máquinas virtuales, filtraciones por canales laterales que exponen chats de IA y spyware que ataca silenciosamente dispositivos Android en la red.



Las señales Wi-Fi podrían ser la clave para el control de acceso sin contacto.

Imagina entrar en un edificio seguro donde la puerta se desbloquea al instante al acercar la mano. Sin tarjetas de acceso, sin PIN, sin huellas dactilares. En cambio, el sistema te identifica por la forma en que tu palma distorsiona la señal Wi-Fi del entorno.

NOTICIAS DE

NUESTROS PARTNERS

Darktrace fue nombrada la única opción de los clientes de Gartner® Peer Insights™ para la detección y respuesta de redes en 2025.

Darktrace ha sido nombrada la única Elección de los Clientes en la encuesta Gartner® Peer Insights™ Voice of the Customer 2025 para Detección y Respuesta de Red, obteniendo una calificación de 4.8/5 de 242 reseñas y siendo nombrada tanto Elección de los Clientes de Gartner como Líder del Cuadrante Mágico.

De la anomalía a la causa raíz en menos de un minuto

Las anomalías indican que algo en tu sistema no funciona como se espera. Detectar estas alertas tempranas brinda a los ingenieros de confiabilidad del sitio (SRE) y a los desarrolladores un margen de tiempo crucial para investigar y resolver el problema antes de que afecte la experiencia del cliente. Sin embargo, la detección por sí sola no basta.

Qué es la detección y respuesta a amenazas de identidad (ITDR) y por qué es importante?

Este blog explora conceptos fundamentales de detección y respuesta a amenazas de identidad, por qué es necesaria y cómo se alinea con la gestión de acceso privilegiado (PAM) y los protocolos de seguridad basados en la identidad, que se están volviendo cada vez más críticos para los mandatos de seguridad como la confianza cero.

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información