BOLETÍN INFORMATIVO N°189

JUNIO 2025

El malware GIFTEDCROOK evoluciona: de ladrón de navegadores a herramienta de recopilación de información

El actor de amenazas detrás del malware GIFTEDCROOK ha realizado actualizaciones importantes para convertir el programa malicioso de un ladrón de datos del navegador básico a una potente herramienta de recopilación de inteligencia.

El FBI advierte sobre la expansión de los ataques de Scattered Spider contra aerolíneas mediante ingeniería social

La Oficina Federal de Investigaciones de Estados Unidos (FBI) ha revelado que ha observado que el notorio grupo de delitos cibernéticos Scattered Spider está ampliando su cobertura para atacar al sector aéreo.

Malware PUBLOAD y Pubshell utilizado en el ataque específico al Tíbet de Mustang Panda

Un actor de amenazas vinculado a China conocido como Mustang Panda ha sido atribuido a una nueva campaña de espionaje cibernético dirigida contra la comunidad tibetana.

MOVEit Transfer enfrenta mayores amenazas a medida que aumentan los escaneos y se atacan las fallas CVE

La empresa de inteligencia de amenazas GreyNoise advierte sobre un "aumento notable" en la actividad de escaneo dirigido a los sistemas Progress MOVEit Transfer a partir del 27 de mayo de 2025, lo que sugiere que los atacantes pueden estar preparándose para otra campaña de explotación masiva o buscando sistemas sin parches.

Vulnerabilidad de preautenticación del servidor MongoDB permite a atacantes activar condición DoS

Se identificó una vulnerabilidad crítica de denegación de servicio de autenticación previa como CVE-2025-6709, que afecta a varias versiones de MongoDB Server en sus ramas de lanzamiento 6.0, 7.0 y 8.0.

Los ciberdelincuentes aprovechan la popularidad de CapCut para recopilar credenciales de Apple ID y datos de tarjetas de crédito.

Los cibercriminales han comenzado a explotar la gran popularidad de CapCut, la aplicación dominante de edición de videos cortos, para orquestar sofisticadas campañas de phishing dirigidas a las credenciales de ID de Apple y a la información de tarjetas de crédito.

RECOMENDACIONES

LECTURA DE SEGURIDAD

¿Estamos protegiendo la IA como el resto de la nube?

En esta entrevista de Help Net Security, Chris McGranahan, Director de Arquitectura e Ingeniería de Seguridad en Backblaze , analiza cómo la IA está transformando las tácticas de ciberseguridad, tanto ofensivas como defensivas.

Resumen semanal: Se encuentra una puerta trasera en dispositivos SOHO con Linux y se corrige una falla de alto riesgo en WinRAR RCE

A continuación se ofrece un resumen de algunas de las noticias, artículos, entrevistas y vídeos más interesantes de la semana pasada.

Qué es lo que realmente importa a los LLM? ¿En qué deberían centrarse los CISO?

En un mercado excesivamente reactivo a los riesgos que plantean los grandes modelos de lenguaje (LLM), los CISO no deben entrar en pánico. Aquí hay cuatro fundamentos de seguridad sensatos para respaldar las operaciones comerciales basadas en IA en toda la empresa.

NOTICIAS DE

NUESTROS PARTNERS

Maximizar la eficiencia de la nube: impulsar la optimización de costos y la sostenibilidad con Dynatrace

A medida que las organizaciones adoptan un futuro basado en la nube y la IA, aumenta la presión para controlar el gasto en infraestructura y, al mismo tiempo, cumplir con los objetivos de sostenibilidad.

Presentamos Maximo Assistant: un recurso de IA para equipos

En IBM, integramos IA en Maximo Application Suite mediante potentes capacidades que automatizan tareas, optimizan flujos de trabajo y mejoran la toma de decisiones. No se trata solo de un asistente inteligente que ofrece información crucial, sino de un enfoque más inteligente y eficiente para la gestión de activos empresariales.

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