BOLETÍN INFORMATIVO N°211

DICIEMBRE 2025

El ransomware VolkLocker fue expuesto mediante una clave maestra codificada que permite un descifrado gratuito.

El grupo hacktivista prorruso conocido como CyberVolk (también conocido como GLORIAMIST) ha resurgido con una nueva oferta de ransomware como servicio (RaaS) llamada VolkLocker que sufre fallas de implementación en los artefactos de prueba, lo que permite a los usuarios descifrar archivos sin pagar una tarifa de extorsión.

Repositorios falsos de GitHub que difunden cargas útiles de malware PyStoreRAT

Los investigadores de ciberseguridad están llamando la atención sobre una nueva campaña que aprovecha los repositorios de Python alojados en GitHub para distribuir un troyano de acceso remoto (RAT) basado en JavaScript no documentado previamente, denominado PyStoreRAT .

Nuevos kits de phishing avanzados utilizan IA y tácticas de evasión de MFA para robar credenciales a gran escala.

Los investigadores de ciberseguridad han documentado cuatro nuevos kits de phishing llamados BlackForce, GhostFrame, InboxPrime AI y Spiderman que son capaces de facilitar el robo de credenciales a gran escala.

Nuevas vulnerabilidades de React RSC permiten ataques de denegación de servicio (DoS) y exposición del código fuente

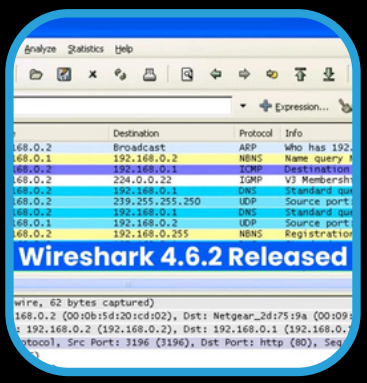
El equipo de React ha publicado correcciones para dos nuevos tipos de fallas en React Server Components (RSC) que, si se explotan con éxito, podrían provocar una denegación de servicio (DoS) o la exposición del código fuente.

Google advierte sobre una vulnerabilidad de día cero en Chrome que se está explotando activamente

Google ha lanzado una actualización de seguridad urgente para el navegador Chrome para abordar una vulnerabilidad de día cero de alta gravedad que actualmente se está explotando.

Wireshark 4.6.2 se lanzó con correcciones para vulnerabilidades y compatibilidad con protocolos actualizada

Wireshark 4.6.2, la última versión del analizador de protocolos de red de código abierto líder, soluciona vulnerabilidades críticas de fallos y problemas de compatibilidad de plugins. Esta versión de mantenimiento prioriza la estabilidad para los usuarios en la resolución de problemas y el análisis de seguridad.



RECOMENDACIONES

LECTURA DE SEGURIDAD

¿Qué tipos de cumplimiento debería soportar su administrador de contraseñas?

La pérdida de credenciales y los controles de autenticación deficientes siguen siendo la causa principal de muchos incidentes de seguridad. Los líderes de TI y los CISO conocen bien este problema. También saben que los reguladores vigilan cómo las organizaciones protegen las contraseñas, rastrean el acceso y documentan las decisiones de seguridad

Resumen semanal: Días cero de Apple, exploit de WinRAR, multas de LastPass, RCE de .NET, estafas de OAuth y más

A continuación, enumeramos las actualizaciones urgentes que debe instalar ahora mismo para detener estas amenazas activas.

NOTICIAS DE

NUESTROS PARTNERS

Cómo Darktrace está poniendo fin a los silos de seguridad del correo electrónico con nuevas capacidades de detección entre dominios, DLP e integraciones nativas de Microsoft

Darktrace está ofreciendo una importante evolución en seguridad de correo electrónico, uniendo verdadera detección entre dominios impulsada por IA, DLP conductual sin etiquetas y automatización nativa de Microsoft para detectar el 17 % de las amenazas que los SEG pasan por alto.

Gestión unificada de la privacidad y datos confidenciales para registros con el Centro de datos confidenciales

Gestionar datos confidenciales en archivos de registro es aún más fácil con Dynatrace. Nuestro nuevo Centro de Datos Sensibles unifica el flujo de trabajo de solicitudes de privacidad, la limpieza de datos y el nuevo Escáner de Datos Sensibles para ayudarle a optimizar el trabajo con datos confidenciales en Dynatrace.

IBM adquirirá Confluent para crear una plataforma de datos inteligentes para la IA generativa empresarial

IBM y Confluent, Inc, empresa pionera en streaming de datos, anunciaron hoy la firma de un acuerdo definitivo por el cual IBM adquirirá la totalidad de las acciones ordinarias emitidas y en circulación de Confluent a un precio de 31 dólares por acción, lo que representa un valor empresarial de 11 000 millones de dólares.

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