BOLETÍN INFORMATIVO N°209

NOVIEMBRE 2025

Un gusano de WhatsApp basado en Python propaga el ladrón Eternidade en dispositivos brasileños

Investigadores de ciberseguridad han revelado detalles de una nueva campaña que aprovecha una combinación de ingeniería social y secuestro de WhatsApp para distribuir un troyano bancario basado en Delphi llamado Eternidade Stealer como parte de ataques dirigidos a usuarios en Brasil.

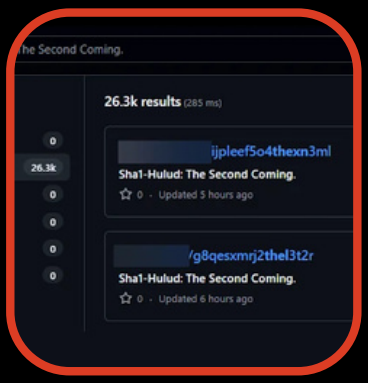
El malware ShadowPad explota activamente una vulnerabilidad de WSUS para obtener acceso completo al sistema

Una falla de seguridad recientemente parcheada en Microsoft Windows Server Update Services (WSUS) ha sido explotada por actores de amenazas para distribuir malware conocido como ShadowPad.

Matrix Push C2 utiliza notificaciones del navegador para ataques de phishing multiplataforma sin archivos

Los actores maliciosos están aprovechando las notificaciones del navegador como vector de ataques de phishing para distribuir enlaces maliciosos mediante una nueva plataforma de comando y control (C2) llamada Matrix Push C2.

La segunda ola de Sha1-Hulud afecta a más de 25.000 repositorios mediante el robo de credenciales de preinstalación de npm



Varios proveedores de seguridad están haciendo sonar la alarma sobre una segunda ola de ataques dirigidos al registro npm de una manera que recuerda al ataque Shai-Hulud .

Google publica una corrección de seguridad para la vulnerabilidad de día cero de Chrome V8 explotada activamente

Google lanzó el lunes actualizaciones de seguridad para su navegador Chrome para corregir dos fallas de seguridad, incluida una que ha sido explotada activamente.

Oracle presuntamente vulnerado por el ransomware Clop mediante un ataque de día cero a E-Business Suite

La famosa banda de ransomware Clop ha incluido a Oracle en su sitio de filtraciones de la dark web, alegando una violación exitosa de los sistemas internos del gigante tecnológico.

Las vulnerabilidades de Wireshark permiten a los atacantes bloquear el sistema al inyectar un paquete mal formado

La Fundación Wireshark ha lanzado una actualización de seguridad crucial para su analizador de protocolo de red ampliamente utilizado, que aborda múltiples vulnerabilidades que podrían provocar condiciones de denegación de servicio.

RECOMENDACIONES

LECTURA DE SEGURIDAD

El cifrado cuántico está llevando el hardware satelital a sus límites

En esta entrevista de Help Net Security, el Coronel Ludovic Monnerat, Comandante del Comando Espacial de las Fuerzas Armadas Suizas , analiza cómo avanza la seguridad de los activos espaciales en respuesta a las amenazas cuánticas emergentes.

Los puntos ciegos del correo electrónico vuelven a afectar a los equipos de seguridad

El panorama de amenazas obliga a los CISO a replantearse lo que consideran normal. El último Informe de Ciberseguridad 2026 de Hornetsecurity, basado en el análisis de más de 70 000 millones de correos electrónicos y una amplia telemetría de amenazas, muestra que los atacantes están adoptando la automatización, la ingeniería social basada en IA y nuevas técnicas de evasión a gran escala.

Resumen semanal: Exploit de Fortinet, ataque de día cero en Chrome, malware BadIIS, DDoS récord, vulneración de SaaS y más

Esta semana se produjeron muchos nuevos problemas cibernéticos. Los hackers atacaron Fortinet y Chrome con nuevos fallos de día cero.

NOTICIAS DE

NUESTROS PARTNERS

Protección de la IA generativa: gestión del riesgo en Amazon Bedrock con Darktrace/CLOUD

Los servicios de IA generativa como Amazon Bedrock presentan nuevos riesgos en cuanto al acceso, la visibilidad y la exposición de datos

Aumente la confiabilidad de la nube: Dynatrace y Azure SRE Agent se unen para operaciones autónomas

La integración de Dynatrace con Microsoft Azure SRE Agent establece un nuevo referente para las operaciones en la nube al aprovechar el análisis de causa raíz basado en IA y la información de producción en tiempo real, junto con una comprensión integral de entornos de TI complejos y a gran escala.

IBM Consulting Advantage se integra con Microsoft Copilot para impulsar flujos de trabajo más inteligentes y rápidos con IA empresarial

A principios de año, compartí mi convicción de que la adopción exitosa de la IA depende de que sea fácil de usar en los procesos y herramientas que los empleados utilizan a diario. Hoy, me complace anunciar que seguimos equipando a los consultores de IBM con el mejor software y las mejores herramientas en todas las plataformas para maximizar la productividad, ahora reforzada por las capacidades combinadas de IBM y Microsoft.

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