BOLETÍN INFORMATIVO N°208

NOVIEMBRE 2025

Dragon Breath utiliza RONINGLOADER para deshabilitar las herramientas de seguridad e implementar el RAT Ghost

Se ha observado que el actor de amenazas conocido como Dragon Breath utiliza un cargador de varias etapas con nombre en clave RONINGLOADER para distribuir una variante modificada de un troyano de acceso remoto llamado Ghost RAT.

La extensión falsa de Chrome "Safery" roba frases semilla de billeteras Ethereum usando la blockchain Sui.

Investigadores de ciberseguridad han descubierto una extensión maliciosa de Chrome que se hace pasar por una billetera Ethereum legítima, pero que alberga funcionalidades para extraer las frases semilla de los usuarios.

RondoDox aprovecha servidores XWiki sin parchear para incorporar más dispositivos a su botnet.

Se ha observado que el malware de botnet conocido como RondoDox ataca instancias de XWiki sin parchear, aprovechando una grave vulnerabilidad de seguridad que podría permitir a los atacantes ejecutar código arbitrario.

Microsoft corrige 63 fallos de seguridad, incluyendo una vulnerabilidad de día cero en el kernel de Windows que está siendo objeto de un ataque activo.

Microsoft publicó el martes parches para 63 nuevas vulnerabilidades de seguridad identificadas en su software, incluyendo una que ha sido explotada activamente en la práctica.

Vulnerabilidad de Fortinet FortiWeb, ahora corregida, explotada en ataques para crear cuentas de administrador.

Los investigadores de ciberseguridad están alertando sobre una vulnerabilidad de omisión de autenticación en el firewall de aplicaciones web (WAF) Fortinet Fortiweb que podría permitir a un atacante tomar el control de las cuentas de administrador y comprometer completamente un dispositivo.

Vulnerabilidad crítica en pgAdmin4 permite a los atacantes ejecutar código remoto en los servidores.

Se ha descubierto una grave vulnerabilidad de ejecución remota de código (RCE) en pgAdmin4, la popular interfaz de código abierto para bases de datos PostgreSQL.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Active Directory bajo ataque: ¿Por qué la infraestructura crítica necesita mayor seguridad?

Active Directory sigue siendo la columna vertebral de la autenticación para más del 90 % de las empresas Fortune 1000. Su importancia ha crecido a medida que las empresas adoptan infraestructuras híbridas y en la nube, pero también su complejidad.

La tecnología que transforma las cadenas de suministro de frágiles a irrompibles

En esta entrevista de Help Net Security, Sev Kelian, CISO y vicepresidente de seguridad de Tecsys , analiza cómo las organizaciones pueden fortalecer la resiliencia de la cadena de suministro mediante una estrategia más unificada y con visión de futuro .

La próxima brecha tecnológica está escrita en la difusión de la IA.

Según un informe de Microsoft, la IA se está extendiendo más rápido que cualquier otra tecnología importante en la historia. Más de 1200 millones de personas han utilizado alguna herramienta de IA en los tres años posteriores a los primeros lanzamientos masivos.

NOTICIAS DE

NUESTROS PARTNERS

Por qué la API y el registro en diario ofrecen una seguridad de correo electrónico más rápida y respaldada por SLA para Microsoft 365?

Descubra cómo la API + el registro de eventos de Darktrace reducen la latencia de detección de amenazas de correo electrónico hasta 30 veces en comparación con el uso exclusivo de API, lo que aumenta la velocidad, la confiabilidad y la resiliencia para Microsoft 365.

Cuadrante Mágico de Gartner® 2025 para la Gestión de Acceso Privilegiado (PAM)

En opinión de BeyondTrust, recibir el reconocimiento como líder durante siete años consecutivos en el Cuadrante Mágico de Gartner® para la Gestión de Acceso Privilegiado valida nuestra continua excelencia en PAM y seguridad de identidad, así como nuestro compromiso para abordar los desafíos de identidad más apremiantes de la actualidad.

IBM presenta nuevos procesadores cuánticos, software y avances algorítmicos en el camino hacia la ventaja y la tolerancia a fallos.

IBM reveló avances fundamentales en su camino para ofrecer tanto una ventaja cuántica para finales de 2026 como computación cuántica tolerante a fallos para 2029

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