BOLETÍN INFORMATIVO N°195

AGOSTO 2025

La filtración del código fuente del troyano bancario ERMAC V3.0 expone toda la infraestructura de malware

Investigadores de ciberseguridad han detallado el funcionamiento interno de un troyano bancario de Android llamado ERMAC 3.0, descubriendo graves deficiencias en la infraestructura de los operadores.

Investigadores detectan una puerta trasera de XZ Utils en docenas de imágenes de Docker Hub, lo que aumenta los riesgos en la cadena de suministro

Una nueva investigación ha descubierto imágenes de Docker en Docker Hub que contienen la infame puerta trasera XZ Utils, más de un año después del descubrimiento del incidente.

Se descubre que piratas informáticos utilizan CrossC2 para expandir el alcance de Cobalt Strike Beacon a Linux y macOS

El centro de coordinación CERT de Japón (JPCERT/CC) reveló el jueves que observó incidentes que involucraron el uso de un marco de comando y control (C2) llamado CrossC2 , que está diseñado para extender la funcionalidad de Cobalt Strike a otras plataformas como Linux y Apple macOS para el control del sistema multiplataforma.

Cisco advierte sobre una falla en CVSS 10.0 FMC RADIUS que permite la ejecución remota de código

Cisco ha publicado actualizaciones de seguridad para abordar una falla de seguridad de máxima gravedad en el software Secure Firewall Management Center (FMC) que podría permitir a un atacante ejecutar código arbitrario en los sistemas afectados.

Vulnerabilidades críticas de PostgreSQL permiten la inyección de código arbitrario durante la restauración

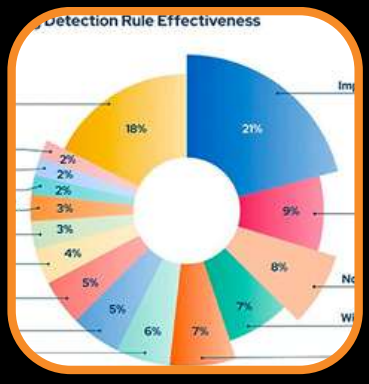
El Grupo de Desarrollo Global de PostgreSQL ha emitido actualizaciones de seguridad de emergencia en todas las versiones compatibles para abordar tres vulnerabilidades críticas que podrían permitir a los atacantes ejecutar código arbitrario durante los procesos de restauración de bases de datos.

Vulnerabilidad en la implementación web de Microsoft IIS permite a los atacantes ejecutar código remoto

Una vulnerabilidad crítica en la herramienta Microsoft Web Deploy podría permitir a atacantes autenticados ejecutar código remoto en los sistemas afectados.

RECOMENDACIONES

LECTURA DE SEGURIDAD



Las alertas débiles y la prevención de errores aumentan los niveles de riesgo para los CISO

La eficacia de la prevención está disminuyendo, las brechas de detección siguen siendo amplias y los atacantes están explotando las vulnerabilidades en la protección de datos y las credenciales.

Cómo los equipos de seguridad están poniendo en práctica la IA en este momento

La IA está pasando de la prueba de concepto a las operaciones de seguridad cotidianas. En muchos SOC, se utiliza para reducir el ruido de alertas , guiar a los analistas durante las investigaciones y agilizar la respuesta a incidentes.

Resumen semanal: Dos actores de amenazas explotan WinRAR de día cero; Microsoft corrige la falla "BadSuccessor" de Kerberos

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

NOTICIAS DE

NUESTROS PARTNERS

Cómo las organizaciones abordan la investigación y la respuesta en la nube

La importancia de la investigación en la nube y la respuesta a incidentes se ve agravada por la mayor superficie de ataque en la nube, la falta de herramientas avanzadas para capacitar a los equipos y la creciente presión regulatoria derivada de las normativas de cumplimiento.

Cómo empoderar a los desarrolladores sin sacrificar la seguridad: un enfoque más inteligente para los derechos de administrador

Revocar los derechos de administrador local es una práctica común de seguridad, pero cuando impide que los desarrolladores realicen su trabajo, genera fricción y riesgo. Una solución de Gestión de Privilegios de Endpoints (EPM) ofrece una solución.

Deja que el problema te guíe: solución inteligente con Dynatrace

Imagina que un amigo te contacta para verte en un nuevo restaurante cuya ubicación desconoces. ¿Saldrías y empezarías a caminar, esperando encontrar el restaurante por pura suerte? Lo más probable es que abras una aplicación de navegación en tu dispositivo móvil, busques la dirección y establezcas tu ruta.

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