Mainsoft®

BOLETÍN INFORMATIVO

#221 | Mayo 2026

Lazarus despliega RemotePE, un troyano de acceso remoto basado únicamente en memoria, contra empresas financieras y de criptomonedas.

Investigadores de ciberseguridad han arrojado luz sobre un malware multiplataforma llamado RemotePE que ha sido utilizado por el Grupo Lazarus, vinculado a Corea del Norte, en ataques dirigidos a organizaciones financieras y de criptomonedas.

ver artículo >>

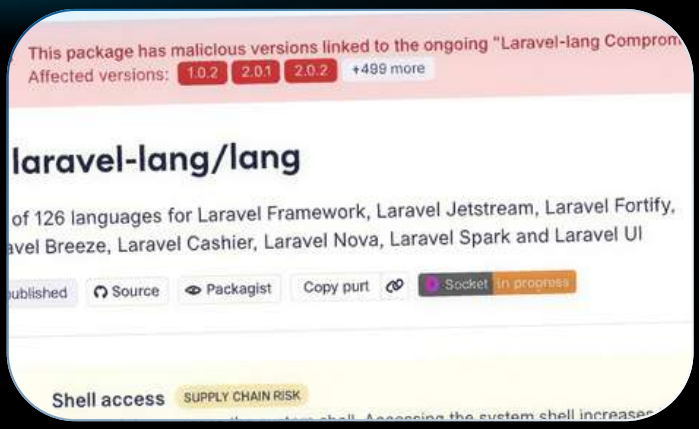
Ataque a la cadena de suministro de Packagist infecta 8 paquetes mediante malware Linux alojado en GitHub.

Una nueva campaña de ataque "coordinada" a la cadena de suministro ha afectado a ocho paquetes en Packagist , incluyendo código malicioso diseñado para ejecutar un binario de Linux obtenido de una URL de lanzamientos de GitHub.

ver artículo >>

Paquetes PHP de Laravel-Lang comprometidos para distribuir un robo de credenciales multiplataforma

Investigadores de ciberseguridad han alertado sobre una nueva campaña de ataques a la cadena de suministro de software que ha tenido como objetivo múltiples paquetes PHP pertenecientes a Laravel-Lang para ofrecer un completo marco de trabajo para el robo de credenciales



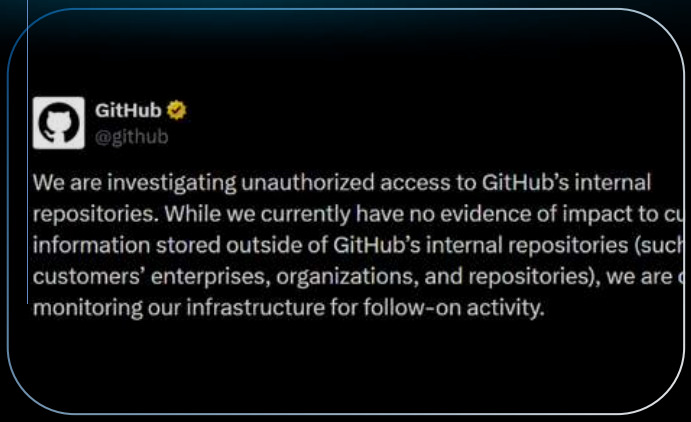
ver artículo >>

INCIDENTES DE SISTEMAS

GitHub sufre una brecha de seguridad: el hackeo de dispositivos de empleados provocó la filtración de más de 3800 repositorios internos.

GitHub anunció el martes que está investigando el acceso no autorizado a sus repositorios internos después de que el conocido ciberdelincuente TeamPCP pusiera a la venta el código fuente de la plataforma y sus organizaciones internas en un foro de ciberdelincuencia.

ver artículo >>



Splunk corrige múltiples vulnerabilidades que permiten ataques DoS y exponen datos confidenciales.

Splunk ha publicado actualizaciones de seguridad que solucionan múltiples vulnerabilidades en Splunk Enterprise , Splunk Cloud Platform y Splunk AI Toolkit, las cuales podrían provocar ataques de denegación de servicio (DoS) y la exposición de datos confidenciales.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Por qué algunas correcciones de seguridad nunca llegan a su panel de vulnerabilidades?

CVE se creó para rastrear fallos de código y sus correcciones. Ahora se está extendiendo para abarcar malware e incidentes en la cadena de suministro que no encajan en su descripción original. La infraestructura de agentes y los activos de IA son donde esta desviación se vuelve estructural.

ver artículo >>

Los investigadores advierten que las claves de API de Google eliminadas siguen funcionando hasta por 23 minutos

Las claves de API de Google son credenciales que permiten a las aplicaciones acceder a los servicios de Google, desde Maps hasta la IA Gemini. Si una clave se filtra, un atacante puede usarla para realizar llamadas a la API, generar cargos y, si Gemini está activado, acceder a los archivos subidos y a las conversaciones almacenadas en caché.

ver artículo >>

Resumen semanal: Fallos de Linux, vulnerabilidades de día cero en Defender, botnets de enrutadores y caos en la cadena de suministro

Resumen del lunes. El mismo desastre, nueva semana.

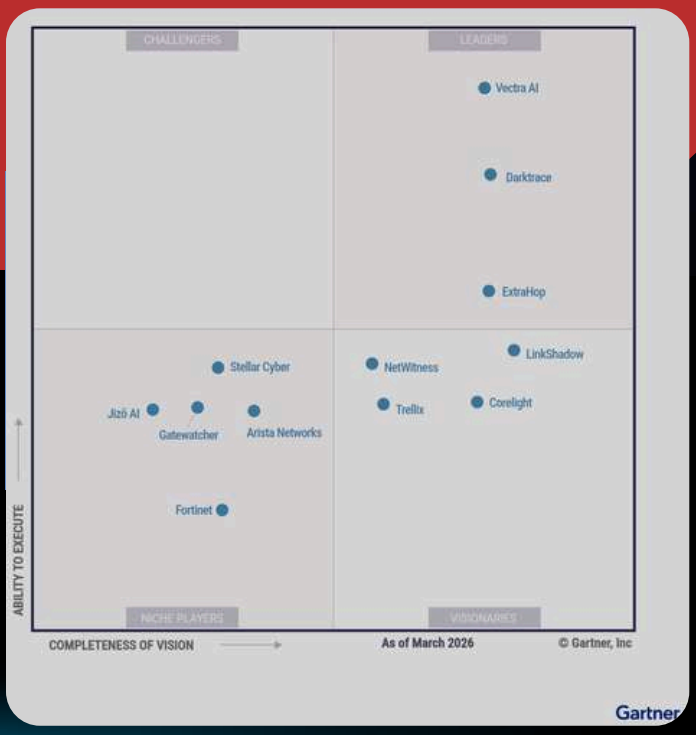
ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Darktrace ha sido nombrada líder en el Cuadrante Mágico™ de Gartner® de 2026 para Detección y Respuesta de Red (NDR) por segundo año consecutivo.

Darktrace ha sido reconocida como líder en el Cuadrante Mágico™ de Gartner® 2026 para Detección y Respuesta de Red (NDR) por segundo año consecutivo. Creemos que esto refleja la excelencia demostrada en NDR, la constante innovación en IA y los excelentes resultados obtenidos para nuestros clientes a nivel mundial.

ver artículo >>



Ampliando el ecosistema de socios para la IA: Novedades de Dynatrace Amplify 2026

La IA está transformando la forma en que las empresas se construyen, operan y escalan. Además, está acelerando la rapidez con la que los socios deben interactuar, diferenciarse y generar valor.

ver artículo >>

Cómo proteger la infraestructura nativa de la nube a gran escala y velocidad: una conversación con Madhu Adireddi

En esta sesión de preguntas y respuestas, Madhu Adireddi, Directora de Gestión de Producto para Acceso Remoto Privilegiado, comparte estrategias para alinear la seguridad con la velocidad de DevOps.

ver artículo >>

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