BOLETÍN INFORMATIVO

Mainsoft

N°173

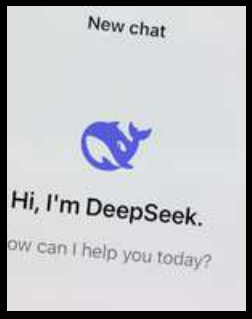
FEBRERO 2025

Las 3 principales amenazas de ransomware activas en 2025

A continuación, desglosamos las tres principales familias de ransomware activas en 2025: LockBit, Lynx y Virlock, y descubrimos cómo el análisis interactivo ayuda a las empresas a detectarlas y detenerlas antes de que sea demasiado tarde.

DragonRank explota servidores IIS con malware BadIIS para fraudes SEO y redireccionamientos de apuestas

Se ha observado que actores de amenazas atacan servidores de Internet Information Services (IIS) en Asia como parte de una campaña de manipulación de optimización de motores de búsqueda (SEO) diseñada para instalar malware BadIIS.



La aplicación DeepSeek transmite datos confidenciales del usuario y del dispositivo sin cifrado

Una nueva auditoría de la aplicación móvil de DeepSeek para el sistema operativo iOS de Apple ha encontrado evidentes problemas de seguridad, el más importante de los cuales es que envía datos confidenciales a través de Internet sin ningún tipo de cifrado, lo que los expone a ataques de interceptación y manipulación.

CISA advierte sobre ataques activos dirigidos contra vulnerabilidad de Trimble Cityworks

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) advirtió que una falla de seguridad que afecta al software de gestión de activos centrado en SIG Trimble Cityworks ha sido objeto de explotación activa.

Cisco fue hackeado: un grupo de ransomware supuestamente vulneró la red interna y obtuvo acceso a AD

Según se informa, Cisco ha sido víctima de una importante violación de datos, y credenciales confidenciales de su red interna y de su infraestructura de dominio se filtraron en línea.

Cisco corrige vulnerabilidades críticas de ISE habilitando Root CmdExec y PrivEsc

Cisco ha publicado actualizaciones para abordar dos fallas de seguridad críticas en Identity Services Engine (ISE) que podrían permitir a atacantes remotos ejecutar comandos arbitrarios y elevar privilegios en dispositivos susceptibles.

Sitios falsos de Google Chrome distribuyen malware ValleyRAT mediante secuestro de DLL

Se han utilizado sitios web falsos que publicitan Google Chrome para distribuir instaladores maliciosos de un troyano de acceso remoto llamado ValleyRAT.

Una vulnerabilidad del kernel de Linux de hace siete años permite a los atacantes ejecutar código remoto

Los investigadores han descubierto una falla crítica en el kernel de Linux que podría permitir a los atacantes ejecutar código remoto.

RECOMENDACIONES

LECTURA DE SEGURIDAD

Resumen semanal: se encontró malware que roba criptomonedas y vulnerabilidad de día cero explotada en 7-Zip en App Store y Google

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

Validación de seguridad: el nuevo estándar para la ciberresiliencia

La validación de seguridad ha dado un giro oficial. Antes se consideraba algo "bueno de tener", pero ahora es una prioridad para los líderes de seguridad de todo el mundo.

El fabricante de etiquetas Avery afirma que la investigación sobre ransomware también encontró un raspador de tarjetas de crédito

El mayor proveedor de etiquetas del mundo dijo que un ataque de ransomware en diciembre provocó una investigación que condujo al descubrimiento de una violación de datos que afectó la información de aproximadamente 67.000 clientes.

NOTICIAS DE

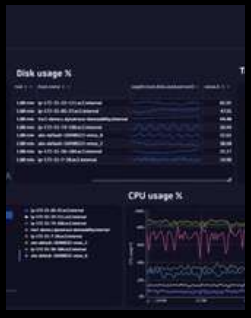
NUESTROS PARTNERS

Reimaginando su SOC: cómo desbloquear un estado de seguridad proactivo

Cómo reinventar su SOC, parte 3/3: Este blog explora los desafíos que enfrentan los profesionales de seguridad al gestionar el riesgo cibernético, evalúa las soluciones actuales del mercado y describe estrategias para desarrollar una postura de seguridad proactiva.

Inteligencia artificial confiable a gran escala: marco de gobernanza y seguridad de la inteligencia artificial de IBM

IBM firmó los compromisos de la Cumbre de Seúl sobre IA para la seguridad de las fronteras de la IA , un paso hacia una IA segura y confiable que IBM ha defendido y promovido durante mucho tiempo. Hoy, publicamos más detalles sobre cómo el marco de gobernanza de la IA de IBM y nuestra cultura organizacional respaldan el desarrollo y el uso responsables de la IA y se alinean con los objetivos centrales de los compromisos de Seúl.



Power Dashboarding, parte I: comience su viaje de exploración con Dashboards

La creación de paneles con plataformas avanzadas de inteligencia y análisis puede resultar intimidante para los usuarios sin experiencia. En Dynatrace, hemos rediseñado por completo nuestro proceso de creación de paneles para que sea fácil para todos lograr resultados rápidos. En esta serie de publicaciones del blog, aprenderá a lograr resultados sorprendentes mediante la creación de paneles interactivos impulsados por IA sin conocimientos previos y comenzando desde cero.

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

CYLANCE — Más Información

IBM Gold Partner — Más Información