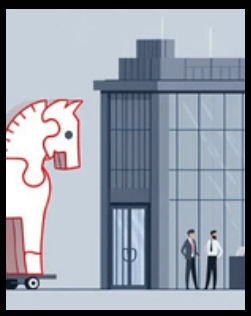
BOLETÍN INFORMATIVO

Mainsoft®

N°179

ABRIL 2025



La mayoría de las extensiones de navegador pueden acceder a datos empresariales confidenciales, según un nuevo informe

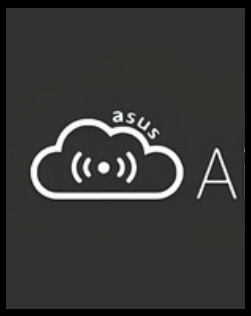
Todo el mundo sabe que las extensiones de navegador están integradas en el flujo de trabajo diario de casi todos los usuarios, desde los correctores ortográficos hasta las herramientas GenAI. Lo que la mayoría de los profesionales de TI y seguridad desconocen es que los permisos excesivos de las extensiones de navegador representan un riesgo creciente para las organizaciones.

Expertos descubren un nuevo controlador e infraestructura XorDDoS a medida que el malware se expande a Docker, Linux e

Los investigadores de ciberseguridad advierten sobre los riesgos continuos que plantea un malware de denegación de servicio distribuido (DDoS) conocido como XorDDoS , con el 71,3 por ciento de los ataques entre noviembre de 2023 y febrero de 2025 dirigidos a Estados Unidos.

Nuevo ataque de ransomware FOG imita a DOGE atacando una organización mediante correo electrónico armado

Investigadores de ciberseguridad han descubierto una sofisticada campaña de ransomware en la que los cibercriminales distribuyen el ransomware FOG mientras persiguen a las víctimas afirmando tener vínculos con el Departamento de Eficiencia Gubernamental (DOGE), una iniciativa reciente del gobierno de EE. UU.



Una vulneASUS confirma falla crítica en enrutadores AiCloud; se insta a los usuarios a actualizar el firmwarerabilidad crítica de PHP permitió a

ASUS ha revelado una falla de seguridad crítica que afecta a los enrutadores con AiCloud habilitado y que podría permitir a atacantes remotos realizar ejecuciones no autorizadas de funciones en dispositivos susceptibles

CISA detecta vulnerabilidades explotadas activamente en dispositivos SonicWall SMA

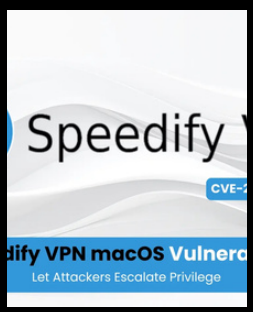
La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) agregó el miércoles una falla de seguridad que afecta a las puertas de enlace SonicWall Secure Mobile Access (SMA) Serie 100 a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), basándose en evidencia de explotación activa.

Apple corrige dos vulnerabilidades de iOS explotadas activamente y utilizadas en sofisticados ataques dirigidos.

Apple lanzó el miércoles actualizaciones de seguridad para iOS, iPadOS, macOS Sequoia, tvOS y visionOS para abordar dos fallas de seguridad que, según dice, han sido objeto de explotación activa.

Vulnerabilidad de Speedify VPN en macOS permite a atacantes escalar privilegios

Se descubrió una vulnerabilidad de seguridad importante, identificada como CVE-2025-25364, en la aplicación macOS de Speedify VPN , que expone a los usuarios a una escalada de privilegios locales y a un compromiso total del sistema.



RECOMENDACIONES

LECTURA DE SEGURIDAD

Resumen semanal: Las alucinaciones de paquetes LLM dañan las cadenas de suministro, se corrigen las fallas del servidor de registro

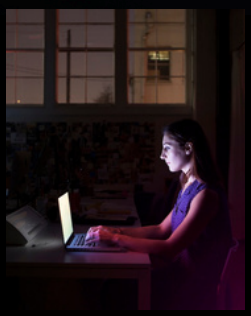
A continuación, se ofrece un resumen de algunas de las noticias, artículos, entrevistas y vídeos más interesantes de la semana pasada.

Los ciberdelincuentes combinan inteligencia artificial e ingeniería social para evitar la detección

Los atacantes se centran cada vez más en el robo de identidades. Por ello, las empresas deben aplicar principios de confianza cero . También deberían verificar la identidad de los usuarios con mayor cuidado, afirma DirectDefense.

NOTICIAS DE

NUESTROS PARTNERS

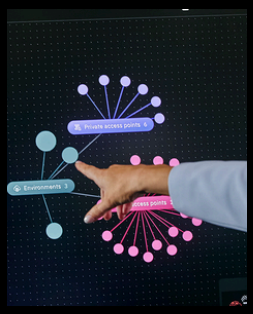


Presentamos la versión 2 del modelo de integración de Darktrace para la investigación de amenazas a la seguridad (DEMIST-2)

Descubra cómo el modelo de integración DEMIST-2 de Darktrace ofrece clasificación y detección de amenazas de alta precisión en cualquier entorno, superando a modelos más grandes con eficiencia y precisión.

Cómo IBM habilita un enfoque holístico para ayudar a mejorar la resiliencia de las aplicaciones con automatización impulsada por IA

Las empresas están inundadas de complejidad, gestionando un promedio de más de 1000 aplicaciones, con menos del 30 % de ellas integradas. Según un artículo de IDC de 2024, se prevé que para 2028 se creen mil millones de nuevas aplicaciones lógicas.



¿Qué solución de seguridad informática es la adecuada para su organización? CSPM vs. KSPM vs. CNAPP

Entre la gran variedad de opciones que ofrece el panorama actual de seguridad en la nube, destacan tres soluciones clave: la Plataforma de Protección de Aplicaciones Nativas de la Nube (CNAPP), la Gestión de la Postura de Seguridad en la Nube (CSPM) y la Gestión de la Postura de Seguridad de Kubernetes (KSPM).

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