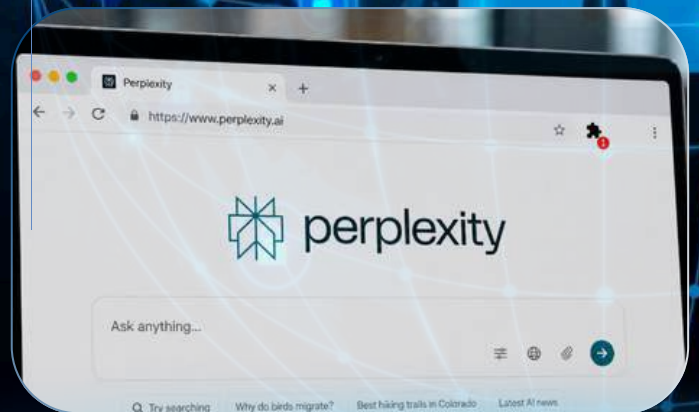


### **La extensión maliciosa Perplexity para Chrome interceptaba búsquedas y la entrada de la barra de direcciones.**

Microsoft ha descubierto una extensión maliciosa para Chrome que se hacía pasar por el motor de búsqueda con inteligencia artificial Perplexity y registraba silenciosamente las búsquedas de los usuarios.

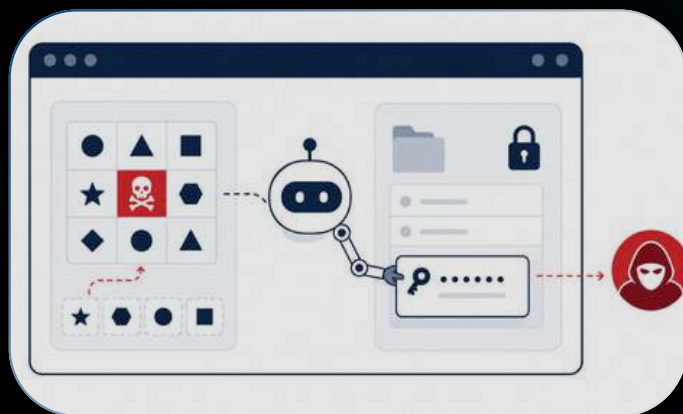
[ver artículo >>](#)



### **Un nuevo y escalofriante ataque biológico engaña a los navegadores de IA para que filtren las credenciales de los usuarios.**

Si convences a un navegador con inteligencia artificial de que está jugando a un videojuego, puede entregar tus datos de inicio de sesión. Este es el descubrimiento detrás de BioShocking, una técnica de la empresa de seguridad LayerX que engañó a seis navegadores y asistentes con IA para que copiaran las credenciales de un usuario y las enviaran a un atacante.

[ver artículo >>](#)



### **El nuevo malware SharkLoader despliega Cobalt Strike en ciberataques de StrikeShark.**

Se ha detectado una campaña de ciberataques recientemente descubierta que distribuye una familia de malware previamente no documentada llamada SharkLoader, la cual actúa como cargador para desplegar Cobalt Strike Beacon en equipos comprometidos.

[ver artículo >>](#)



# INCIDENTES DE SISTEMAS



ORACLE

**Vulnerabilidad CVE-2026-46817 de Oracle E-Business Suite está siendo explotada activamente.**

Según Defused Cyber, una vulnerabilidad de seguridad crítica que afecta a Oracle E-Business Suite está siendo explotada activamente.

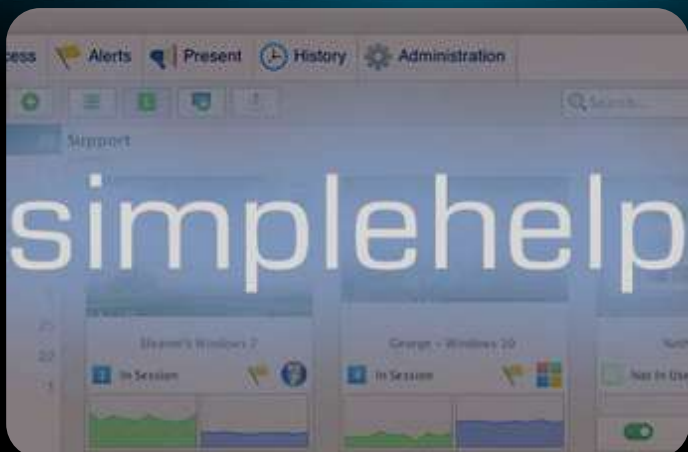
[ver artículo >>](#)



**Se ha publicado una prueba de concepto pública para la vulnerabilidad de ejecución remota de código (RCE) por deserialización en Splunk Secure Gateway.**

Se ha publicado una prueba de concepto pública (PoC) para la vulnerabilidad CVE-2026-20251, una vulnerabilidad de ejecución remota de código (RCE) de alta gravedad que afecta a Splunk Secure Gateway (SSG).

[ver artículo >>](#)



**Vulnerabilidad de SimpleHelp explotada para distribuir el poderoso Djinn Stealer (CVE-2026-48558)**

Los atacantes están explotando la vulnerabilidad CVE-2026-48558, una vulnerabilidad de omisión de autenticación recientemente parcheada en SimpleHelp RMM, para instalar el nuevo malware Djinn Stealer en los ordenadores de las víctimas.

[ver artículo >>](#)

# RECOMENDACIONES DE LECTURA DE SEGURIDAD



**Resumen semanal: Fallos del kernel de Linux, trucos de malware con IA, puerta trasera Turla, ladrones de información y más.**

Esta semana nos recordó que los atacantes no siempre necesitan grandes trucos. Un pequeño error, una antigua ruta de acceso, un parche omitido, y de repente la puerta queda abierta

[ver artículo >>](#)

**Repensar el equilibrio entre la supervisión de la IA y la innovación.**

Los CIOs se enfrentan a una presión creciente para impulsar la adopción de la IA con rapidez, pero ¿a qué precio? Los líderes de TI explican cómo están equilibrando la supervisión y la innovación.

[ver artículo >>](#)



# NOTICIAS DE NUESTROS PARTNERS



## **Cómo Darktrace transformó la ciberseguridad en nuestro centro de salud: la perspectiva de un CIO**

El CIO del sector sanitario explica cómo la integración de Darktrace con la seguridad de Microsoft mejoró la visibilidad, redujo el riesgo y minimizó la carga operativa

[ver artículo >>](#)



## **Cumplimiento de HIPAA en entornos multicloud para el sector sanitario: Dynatrace ahora es compatible con AWS, Azure y GCP.**

Dynatrace ahora ofrece observabilidad compatible con HIPAA para organizaciones de atención médica de EE. UU. en los principales proveedores de nube: AWS, Microsoft Azure y GCP.

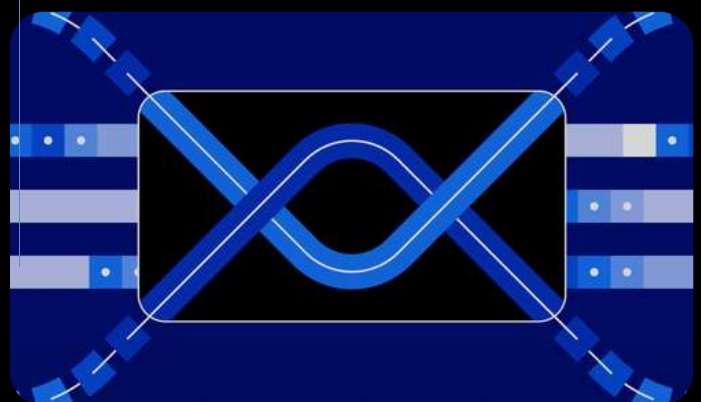
[ver artículo >>](#)



## **IBM, Red Hat y Palo Alto Networks amplían el proyecto Lightwell para ayudar a las organizaciones a responder a las vulnerabilidades del software.**

Palo Alto Networks (NASDAQ: PANW), IBM (NYSE: IBM) y Red Hat anunciaron hoy una colaboración para ayudar a las organizaciones a identificar vulnerabilidades de forma temprana e implementar protecciones rápidamente en software de código abierto, aplicaciones comerciales, tecnología operativa (OT) y tecnologías sanitarias

[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](#)