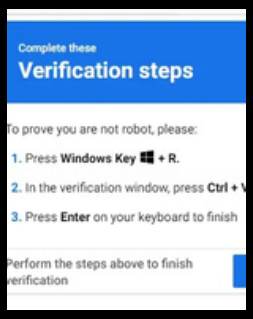
BOLETÍN INFORMATIVO

Mainsoft®

N°185

JUNIO 2025



El nuevo malware EDDIESTEALER elude el cifrado de la aplicación de Chrome para robar datos del navegador.

Una nueva campaña de malware está distribuyendo un novedoso ladrón de información basado en Rust llamado EDDIESTEALER utilizando la popular táctica de ingeniería social ClickFix iniciada a través de páginas de verificación CAPTCHA falsas.

Hackers vinculados a China explotan vulnerabilidades de SAP y SQL Server en ataques en Asia y Brasil

El actor de amenazas vinculado a China que está detrás de la reciente explotación in situ de una falla de seguridad crítica en SAP NetWeaver ha sido atribuido a un conjunto más amplio de ataques dirigidos a organizaciones en Brasil, India y el sudeste asiático desde 2023.

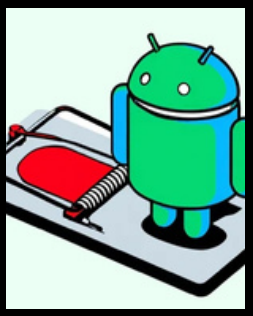
ConnectWise sufre un ciberataque; se sospecha que un actor de un Estado-nación está involucrado en una vulneración selectiva

ConnectWise, el desarrollador del software de acceso y soporte remoto ScreenConnect, ha revelado que fue víctima de un ciberataque que, según dijo, probablemente fue perpetrado por un actor de amenazas de un estado nacional.

Una falla en el selector de archivos de Microsoft OneDrive otorga a las aplicaciones acceso completo a la nube, incluso al cargar un

Investigadores de ciberseguridad han descubierto una falla de seguridad en el Selector de archivos OneDrive de Microsoft que, si se explota con éxito, podría permitir que los sitios web accedan a todo el contenido de almacenamiento en la nube de un usuario, en lugar de solo a los archivos seleccionados para cargar a través de la herramienta.

INCIDENTES DE SISTEMAS



Qualcomm corrige tres vulnerabilidades de día cero utilizadas en ataques dirigidos a Android mediante la GPU Adreno

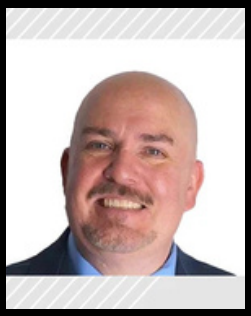
Qualcomm ha enviado actualizaciones de seguridad para abordar tres vulnerabilidades de día cero que, según afirma, han sido explotadas en ataques limitados y dirigidos.

Nuevas fallas de Linux permiten el robo de hash de contraseñas mediante volcados de núcleo en Ubuntu, RHEL y Fedora

Según la Unidad de investigación de amenazas de Qualys (TRU), se han identificado dos fallas de divulgación de información en apport y systemd-coredump , los controladores de volcado de núcleo de Ubuntu, Red Hat Enterprise Linux y Fedora.

RECOMENDACIONES

LECTURA DE SEGURIDAD

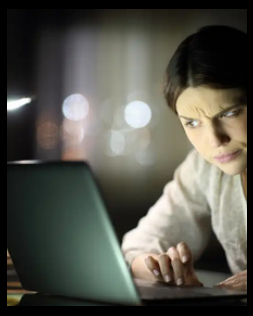


CISO 3.0: Liderando la gobernanza y la seguridad de la IA en la sala de juntas

En esta entrevista de Help Net Security, Aaron McCray, CISO de campo en CDW , analiza cómo la IA está transformando el rol del CISO, pasando de ser un simple guardián de la ciberseguridad táctica a un asesor estratégico de riesgos empresariales. Con la IA integrada en todas las funciones empresariales, los CISO lideran las iniciativas de gobernanza y gestión de riesgos a nivel empresarial.

'Correo electrónico seguro': una batalla perdida que los CISO deben abandonar

En términos de seguridad, el correo electrónico ha sido durante mucho tiempo un modo de comunicación obsoleto en nuestro mundo cada vez más amenazado por la ciberseguridad. Es hora de decir adiós a la ilusión de seguridad del SMTP.



Resumen semanal: NIST propone una nueva métrica de vulnerabilidades y fallas en el software de código abierto de la NASA

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

NOTICIAS DE

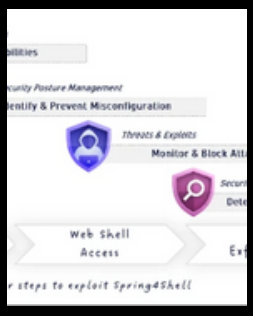
NUESTROS PARTNERS

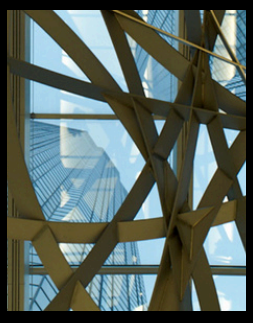
Por qué los enfoques de seguridad del correo electrónico centrados en ataques no pueden hacer frente a las amenazas modernas

A pesar de la evolución de las amenazas del correo electrónico, muchas organizaciones aún dependen de SEG o métodos obsoletos y centrados en ataques. Estos enfoques no pueden contrarrestar los ataques avanzados basados en IA. ¿La solución? Una seguridad del correo electrónico centrada en el negocio que comprenda a los usuarios y el comportamiento de la bandeja de entrada, no solo las amenazas.

Revisando Spring4Shell: Cómo la detección y respuesta de aplicaciones en la nube (CADR) ofrece protección multicapa

Proteger las aplicaciones que se ejecutan en entornos nativos de la nube es una prioridad para muchos profesionales de la seguridad. Para mantenerse al día con el creciente número de amenazas que afectan a las cargas de trabajo en la nube, es fundamental ofrecer protección multicapa mediante la integración fluida de visibilidad, análisis y respuesta en una sola plataforma.





Deutsche Bank acelera la transformación digital con la cartera de software de IBM

El nuevo acuerdo de licencia brinda a Deutsche Bank un mayor acceso a las innovadoras soluciones de software de IBM para acelerar la innovación, optimizar las operaciones y mejorar la experiencia del cliente.

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