BOLETÍN INFORMATIVO

Mainsoft®

N°187

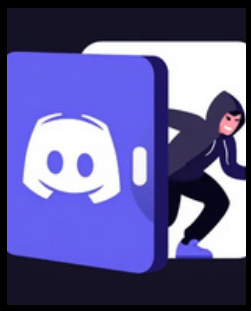
JUNIO 2025

El ransomware Anubis cifra y borra archivos, lo que hace imposible recuperarlos incluso después del pago.

Se ha descubierto una cepa emergente de ransomware que incorpora capacidades para cifrar archivos y borrarlos de forma permanente, un desarrollo que se ha descrito como una "rara amenaza dual".

El secuestro de enlaces de invitación de Discord permite que AsyncRAT y Skuld Stealer ataquen las billeteras de criptomonedas.

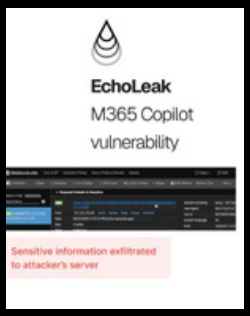
Una nueva campaña de malware está explotando una debilidad en el sistema de invitaciones de Discord para distribuir un ladrón de información llamado Skuld y el troyano de acceso remoto AsyncRAT .



El nuevo ataque TokenBreak elude la moderación de la IA con cambios de texto de un solo carácter.

Los investigadores de ciberseguridad han descubierto una novedosa técnica de ataque llamada TokenBreak que se puede utilizar para eludir las barreras de seguridad y moderación de contenido de un modelo de lenguaje grande (LLM) con un solo cambio de carácter.

INCIDENTES DE SISTEMAS

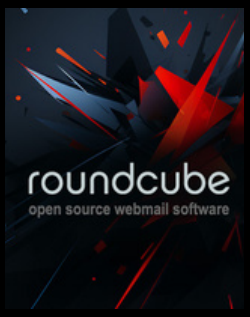


Una vulnerabilidad de IA de clic cero expone los datos de Microsoft 365 Copilot sin interacción del usuario

Una nueva técnica de ataque denominada EchoLeak se ha caracterizado como una vulnerabilidad de inteligencia artificial (IA) de "cero clic" que permite a los actores maliciosos extraer datos confidenciales del contexto de Microsoft 365 (M365) Copilot sin interacción alguna del usuario

Los piratas informáticos suben paquetes maliciosos a los repositorios de PyPI para robar datos de AWS, CI/CD y macOS

Ha surgido una sofisticada campaña de malware dirigida al repositorio Python Package Index (PyPI), en la que los ciberdelincuentes implementan paquetes armados diseñados para robar credenciales confidenciales de infraestructura en la nube y datos corporativos.



Una vulnerabilidad en los servicios de copia de seguridad de IBM permite a los atacantes escalar privilegios

Una vulnerabilidad de seguridad crítica en IBM Backup, Recovery, and Media Services para la plataforma i que podría permitir a los atacantes obtener privilegios elevados y ejecutar código malicioso con acceso a nivel de componente al sistema operativo host.

RECOMENDACIONES

LECTURA DE SEGURIDAD

MDEAutomator: Gestión de endpoints de código abierto, respuesta a incidentes en MDE

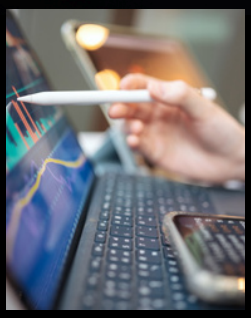
Administrar endpoints y responder a incidentes de seguridad en Microsoft Defender for Endpoint (MDE) puede ser una tarea compleja y que requiere mucho tiempo. MDEAutomator es una herramienta de código abierto diseñada para facilitarlo.

Las estafas de secuestro virtual se aprovechan de nuestros peores miedos

Recibir una llamada diciendo que un familiar ha sido secuestrado es aterrador. El miedo y el pánico se apoderan de la persona, impidiendo pensar con claridad. Eso es precisamente lo que buscan los delincuentes cuando usan una estafa llamada secuestro virtual.

NOTICIAS DE

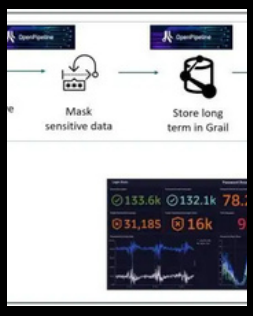
NUESTROS PARTNERS



Rompiendo silos: Por qué la seguridad unificada es crucial en un mundo híbrido

A pesar de la creciente popularidad de los entornos híbridos, la mayoría de las organizaciones enfrentan desafíos para lograr una visibilidad unificada entre las redes locales y en la nube. Las herramientas de plataforma basadas en IA pueden reducir esta brecha de visibilidad para reducir los tiempos de detección y respuesta, y simplificar las operaciones.

Monitoreo de Auth0 con Dynatrace para autenticaciones más seguras



Comprender los patrones de autenticación de usuarios y los eventos de seguridad es fundamental para mantener una seguridad robusta en las aplicaciones. Auth0, líder en gestión de identidades, es una plataforma de identidades segura y personalizable que simplifica la autenticación y la autorización para aplicaciones de cualquier escala. Auth0 genera registros detallados que detallan cada evento de autenticación.

Cuando el Clickbait sale mal: cómo proteger su identidad y su negocio de las estafas de phishing de Clickbait

Las estafas de phishing clickbait explotan desencadenantes emocionales como la curiosidad o el miedo para engañar a los usuarios y hacer que hagan clic en enlaces maliciosos. Este blog, actualizado con estrategias de higiene de ciberseguridad, detalla defensas prácticas, desde técnicas de detección de enlaces y protocolos de informes hasta la limitación de privilegios de administrador y la aplicación oportuna de parches.

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