Mainsoft®

BOLETÍN INFORMATIVO

#218 | Mayo 2026

Grupos de ciberdelincuentes utilizan el vishing y el abuso de SSO en ataques rápidos de extorsión a empresas SaaS.

Investigadores de ciberseguridad alertan sobre dos grupos de ciberdelincuentes que están llevando a cabo "ataques rápidos y de gran impacto" operando prácticamente dentro de los límites de los entornos SaaS, dejando mínimas huellas de sus acciones.

ver artículo >>

Una nueva puerta trasera en Python utiliza un servicio de tunelización para robar credenciales de navegador y de la nube.

Investigadores de ciberseguridad han revelado detalles de un marco de puerta trasera sigiloso basado en Python llamado DEEP#DOOR , que cuenta con capacidades para establecer acceso persistente y recopilar una amplia gama de información confidencial de los hosts comprometidos.

ver artículo >>

Suplantación de identidad de herramientas administrativas de distribución EtherRAT a través de fachadas de GitHub

En marzo de 2026, el Centro de Investigación de Amenazas (TRC) de Atos identificó una sofisticada campaña maliciosa de alta resistencia.

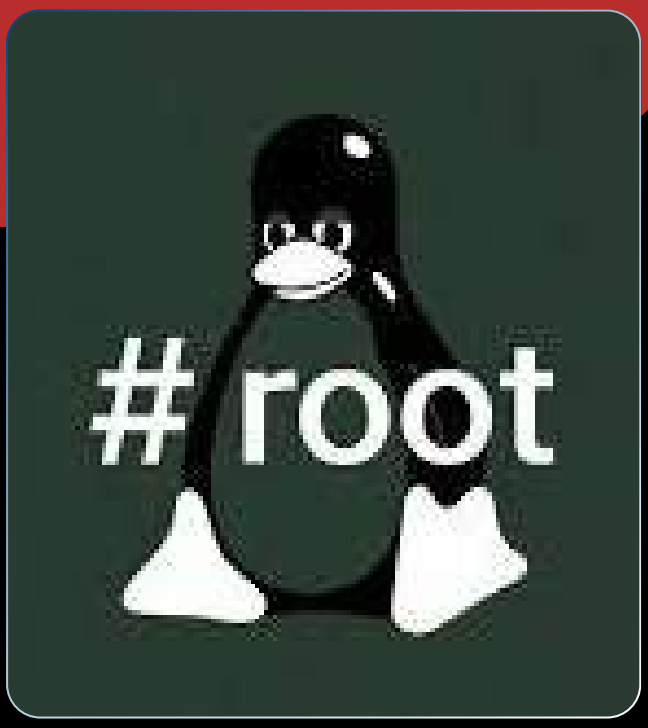
ver artículo >>

INCIDENTES DE SISTEMAS

Se ha identificado una vulnerabilidad crítica en la autenticación de cPanel: actualice su servidor de inmediato.

cPanel ha publicado actualizaciones de seguridad para solucionar un problema de seguridad que afecta a varias rutas de autenticación y que podría permitir a un atacante obtener acceso al software del panel de control.

ver artículo >>



Una nueva vulnerabilidad de Linux denominada 'Error de copia' permite el acceso de administrador en las principales distribuciones.

Investigadores de ciberseguridad han revelado detalles de una vulnerabilidad de escalada de privilegios locales (LPE, por sus siglas en inglés) en Linux que podría permitir que un usuario local sin privilegios obtenga acceso de administrador (root).

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

Un estudio de Okta revela que los agentes de IA pueden eludir las medidas de seguridad y poner en riesgo las credenciales.

El riesgo que suponen las plataformas basadas en agentes, como OpenClaw, es un problema oculto dentro de las empresas.

ver artículo >>

Resumen semanal: Phishing con IA, herramienta de espionaje para Android, exploit para Linux, RCE de GitHub y más.

Mientras la mayoría de los equipos aún estaban clasificando las alertas del mes pasado, los atacantes ya habían convertido los paneles de control en interruptores de apagado, los núcleos en puertas abiertas y las canalizaciones de código abierto en sistemas de entrega silenciosos.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS

Dominando la superficie de ataque moderna: un resumen de las innovaciones en Identity Security Insights del primer trimestre.

En el primer trimestre de 2026, el panorama de la gestión de identidades continúa evolucionando hacia una rápida adopción de la IA y rutas de privilegios cada vez más complejas.

ver artículo >>

Cómo los ataques de inyección de mensajes enviados por correo electrónico pueden atacar la IA empresarial y por qué es importante.

La inyección instantánea es una amenaza emergente, con solo un puñado de víctimas confirmadas hasta el momento, que se centra en cómo los sistemas de IA utilizan los datos en lugar de explotar las vulnerabilidades de software tradicionales.

ver artículo >>

Dynatrace amplía la monitorización de agentes de codificación de IA para Claude Code, Google Gemini CLI, Codex CLI, OpenCode y GitHub Copilot SDK.

Los agentes de codificación basados en IA son fundamentales para que los equipos de ingeniería modernos desarrollen, revisen, implementen y solucionen problemas de software.

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