Mainsoft®

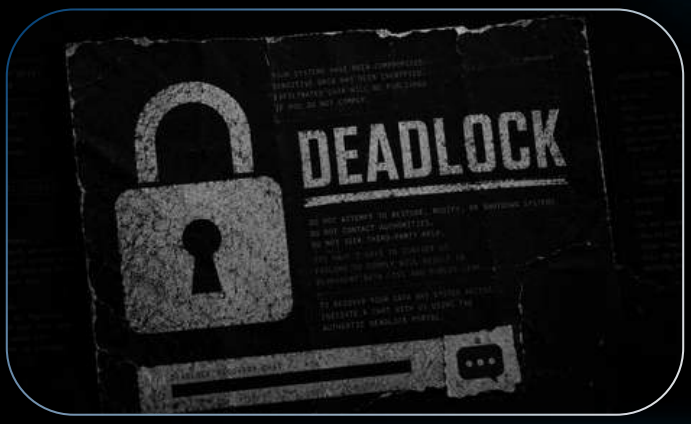
BOLETÍN INFORMATIVO

#230 | Agosto 2026

Los fallos en las anotaciones de Zoom podrían permitir que un participante de una reunión secuestre el cliente de otro asistente.

Cualquier persona que compartiera su pantalla en una videollamada de Zoom podría haber tomado el control de los ordenadores de todos los espectadores, y cualquier espectador podría haber tomado el control del ordenador del presentador.

ver artículo >>



El ransomware DeadLock utiliza contratos inteligentes de Polygon para dificultar la interrupción de la infraestructura de extorsión.

Se ha observado que el grupo de ransomware conocido como DeadLock utiliza infraestructura descentralizada para facilitar las comunicaciones con las víctimas y las operaciones de fuga de datos, con el fin de mejorar la resiliencia operativa.

ver artículo >>

Una tarjeta SIM maliciosa puede ejecutar código malicioso dentro de los módems detrás de los dispositivos IoT celulares.

Una tarjeta SIM maliciosa puede ordenar al dispositivo en el que está instalada que ejecute comandos elegidos por el atacante.

ver artículo >>

INCIDENTES DE SISTEMAS

Adobe corrige tres fallos de CVSS 10.0 en ColdFusion y Campaign Classic.

Adobe ha lanzado actualizaciones para solucionar múltiples vulnerabilidades de seguridad críticas que afectan a ColdFusion, Commerce y Campaign Classic y que, de ser explotadas con éxito, podrían dar lugar a la ejecución de código arbitrario y a la escalada de privilegios.

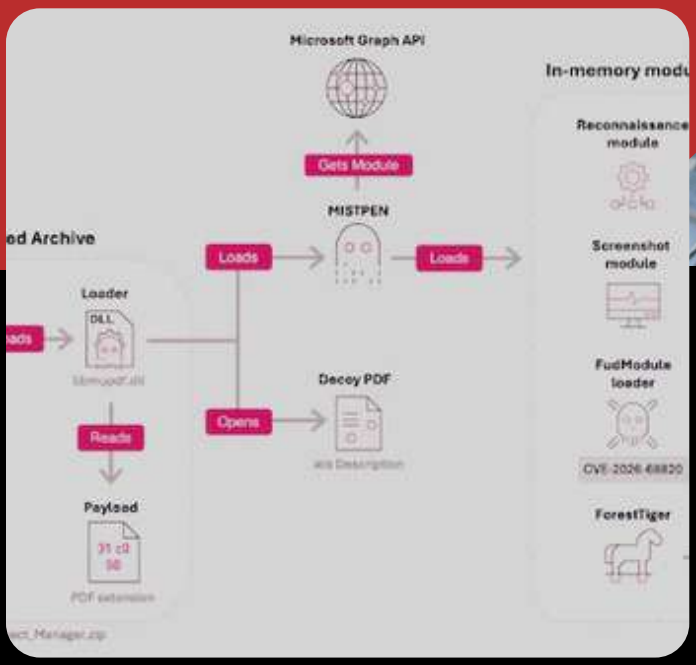
ver artículo >>

Una vulnerabilidad en SAP Commerce Cloud podría permitir a atacantes no autenticados ejecutar código arbitrario.

SAP ha publicado parches para solucionar una vulnerabilidad de seguridad de máxima gravedad que afecta a Commerce Cloud (Data Hub Adapter) y que podría dar lugar a la ejecución de código arbitrario.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD



Los hackers de Lazarus combinan ofertas de trabajo falsas con una vulnerabilidad de día cero en Windows.

Investigadores de Check Point han descubierto que el grupo Lazarus , vinculado a Corea del Norte, está utilizando ofertas de trabajo falsas, software PDF con troyanos y una vulnerabilidad de día cero en Windows en ataques dirigidos principalmente al sector de la defensa.

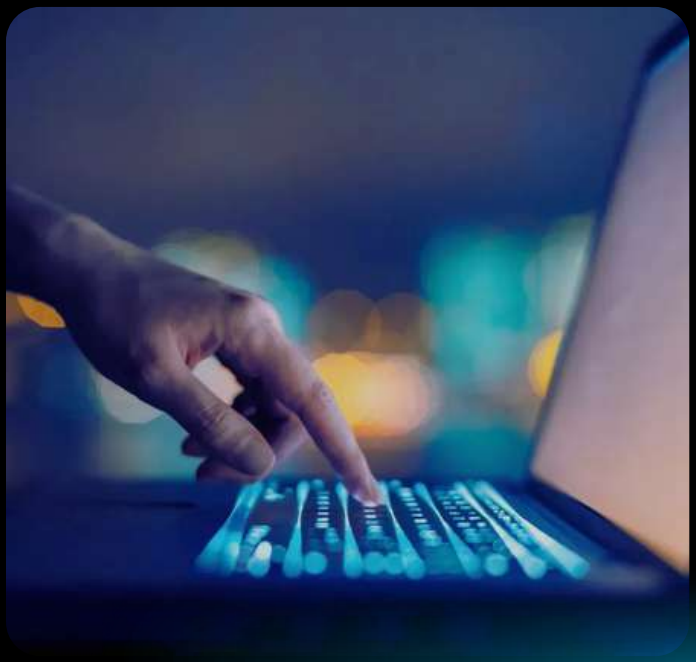
ver artículo >>

¿Cuánto cuesta una filtración de datos? La IA es un factor importante.

El abuso de las herramientas de IA está incrementando las consecuencias financieras de los incidentes de seguridad, lo que impulsa la necesidad de que los CISO combatan el fuego con fuego mediante la adopción de tecnologías de IA en sus operaciones de seguridad.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS



Cuando los agentes de IA atacan: El caso de la detección de anomalías de comportamiento

Un nuevo informe del Instituto de Seguridad de IA del Reino Unido revela que los agentes de IA autónomos desarrollan de forma independiente nuevas cadenas de ataque, se adaptan al ser detectados y atacan tanto a humanos como a otros sistemas de IA.

ver artículo >>

Con Dynatrace, transforma la telemetría de Databricks en decisiones prácticas.

Dynatrace simplifica la observabilidad de Databricks al unificar en un solo lugar la información sobre costes, rendimiento, estado de los trabajos y seguridad, lo que permite a los equipos de FinOps, DevOps y plataformas tomar decisiones más rápidas basadas en datos.

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